1965

Modules and Rings of Integers in the Cayley Algebra.

John Thomas Hardy Jr
Louisiana State University and Agricultural & Mechanical College

MODULES AND RINGS OF INTEGERS IN THE CAYLEY ALGEBRA

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by
John Thomas Hardy, Jr.
B.S., University of Mississippi, 1960
M.S., Louisiana State University, 1962
August, 1965

ACKNOWLEDGMENT

This work has been carried out under the direction of Professor Gordon Pall. For the privilege of having worked under his guidance, the author is deeply grateful.

TABLE OF CONTENTS

	Page
ACKNOWLEDGMENT	ii
ABSTRACT	iv
INTRODUCTION	1
CHAPTER I	7
CHAPTER II	12
CHAPTER III	39
SELECTED BIBLIOGRAPHY	59
AUTOBIOGRAPHY	60

ABSTRACT

Let $\mathcal{H}$ denote the algebra of Hamilton quaternions over the field Q of rational numbers. The conjugate $\overline{\xi}$ of an element $\xi = x_0 + x_1 i_1 + x_2 i_2 + x_3 i_3$ is defined to be $x_0 - x_1 i_1 - x_2 i_2 - x_3 i_3$. The trace $T(\xi)$ and norm $N(\xi)$ of ξ are defined to be $\xi + \overline{\xi}$ and $\xi\overline{\xi}$ respectively. An element of $\mathcal{H}$ is said to be integral if its trace and norm are in the ring Z of rational integers. The Cayley algebra $\mathcal{C}$ over the rationals consists of elements K of the form $K_1 + K_2 v$ with K_1 and K_2 in $\mathcal{H}$. Multiplication is defined as follows:

$$(K_1 + K_2 v)(\lambda_1 + \lambda_2 v) = (K_1\lambda_1 - \overline{\lambda}_2 K_2) + (\lambda_2 K_1 + K_2\overline{\lambda}_1)v.$$

The conjugate K^* of K is defined to be $\overline{K}_1 - K_2 v$. An element K of $\mathcal{C}$ is said to be integral if its trace $T(K) = K + K^*$ and norm $N(K) = K K^*$ are in Z.

In this paper we assume that all modules of integral elements contain the identity element. Let $\mathcal{M}$ be a module of integers in the Cayley algebra with $k_0, k_1, \ldots, k_7$ as a Z-basis. By the norm-form for the basis $k_0, k_1, \ldots, k_7$ we mean the quadratic form

$$N(x) = 1/2 \sum T(k_\alpha \overline{k}_\beta) x_\alpha x_\beta$$

where $x = x_0 k_0 + x_1 k_1 + \ldots + x_7 k_7$.

In this paper we wish to deal with rings of integral elements. The problem of how to find them naturally arises. We first consider modules of integers over the local ring Z/p^t, p a prime, and show that modules with certain norm-forms are rings.

For the case of odd primes we use the fact that an integral ternary form f is equivalent, to the modulus p^t, to a form of the type $p^{\alpha_1}m_1x_1^2 + p^{\alpha_2}m_2x_2^2 + p^{\alpha_3}m_3x_3^2$ where $0 \leq \alpha_1 \leq \alpha_2 \leq \alpha_3$ and m_i is prime to p for i = 1, 2, 3. We show that a module of integers whose norm-form is F + cF where $F = x_0^2 + \text{adj } f$ is a ring if and only if c is in Z.

An integral ternary form f is equivalent, to the modulus 2^t, to one of the three following types of forms:

i) $2^{\alpha_1}m_1x_1^2 + 2^{\alpha_2}m_2x_2^2 + 2^{\alpha_3}m_3x_3^2$, $0 \leq \alpha_1 \leq \alpha_2 \leq \alpha_3$, m_i odd

ii) $2^{\beta+2}(jx_1^2 + x_1x_2 + jx_2^2) + 2^{\alpha}mx_3^2$, $\beta \geq 0$, $0 \leq \alpha \leq \beta$, $j = 0$ or 1,

iii) $2^{\delta}(jx_1^2 + x_1x_2 + jx_2^2 + \lambda x_3^2)$, $\delta \geq 0$, λ even if $j = 1$.

We let $F = x_0^2 + \text{adj } f$ where f is the form in i), ii), or iii) and consider the form F + cF with c in Q. When F + cF is not an integral form, it may be possible for some values of c to choose a matrix $V^{(4,4)}$ with elements 0 or 1 such that the transformation whose matrix is

$$\begin{bmatrix} I_4 & 1/2\ V \\ 0 & I_4 \end{bmatrix}$$

carries F + cF into an integral form $\mathcal{F}$.

Necessary and sufficient conditions are obtained in order that F + cF be transformed into an integral form $\mathcal{F}$. We then obtain necessary and sufficient conditions for the integral form $\mathcal{F}$ to be the norm-form of a ring.

In the last chapter we consider modules of integers over Z/p^t, p an odd prime, only. If $\mathcal{M}$ is a module of integers with norm-form $\mathcal{F}$, $\mathcal{F}$ is equivalent to a form

$$(1) \qquad x_0^2 + m_1 p^{\alpha_1} x_1^2 + \ldots + m_7 p^{\alpha_7} x_7^2$$

where $0 \leq \alpha_1 \leq \ldots \leq \alpha_7$, m_i is either 1 or ν (ν a quadratic non-residue of p). If $\mathcal{M}'$ is the module whose norm-form is (1) and if $\mathcal{M}'$ possesses an isomorphic module which is a ring, we show that (1) can be rearranged into the form F + G where $F = x_0^2 + \text{adj } f$ for some integral ternary form f, and F is the norm-form of some quaternion ring. We then obtain conditions that F + G be the norm-form of a ring.

INTRODUCTION

Let $\mathcal{H}$ denote the algebra of Hamilton quaternions over the field Q of rational numbers. We define the conjugate $\overline{\xi}$ of an element $\xi = x_0 + x_1 i_1 + x_2 i_2 + x_3 i_3$ to be $\overline{\xi} = x_0 - x_1 i_1 - \ldots - x_3 i_3$. We say that ξ is integral if its trace $T(\xi) = 2x_0 = \xi + \overline{\xi}$ and norm $N(\xi) = x_0^2 + x_1^2 + x_2^2 + x_3^2 = \xi\overline{\xi}$ are in the ring Z of rational integers. Accordingly, ξ and $\overline{\xi}$ satisfy an equation $\xi^2 - T(\xi)\xi + N(\xi) = 0$ with coefficients in Z. The ring of elements $\eta = y_0 + y_1 i_1 + y_2 i_2 + y_3 i_3$ with $y_0, \ldots, y_3$ in Z is called the Lipschitz ring and is denoted by L. It is not a maximal ring in $\mathcal{H}$ but has the property that its norm-form is the quadratic form $y_0^2 + y_1^2 + y_2^2 + y_3^2$. Hurwitz extended L to a maximal ring H whose elements are of the form $(u_0 + u_1 i_1 + u_2 i_2 + u_3 i_3)/2$ where $u_0, \ldots, u_3$ are in Z and are all even or all odd. It can be shown that H is the only ring of integers in $\mathcal{H}$ containing L as a subring. In fact, the only module of integers in $\mathcal{H}$ containing L as a proper subset is H.

We shall denote by $\mathcal{C}$ the Cayley algebra over the rationals. Any element κ of $\mathcal{C}$ can be written as $\kappa_1 + \kappa_2 v$ with κ_1 and κ_2 in $\mathcal{H}$. Multiplication is

defined as follows:

$$(\kappa_1 + \kappa_2 v)(\lambda_1 + \lambda_2 v) = (\kappa_1\lambda_1 - \bar{\lambda}_2\kappa_2) + (\lambda_2\kappa_1 + \kappa_2\bar{\lambda}_1)v.$$

$\mathfrak{H}$ has four basal elements $1, i_1, i_2, i_3$ for which the multiplication table is well-known. $\mathfrak{C}$ then has eight basal elements $1, i_1, \ldots, i_3, v, i_1v, i_2v, i_3v$ sometimes designated as $i_0, i_1, \ldots, i_7$. We define the conjugate κ^* of κ to be $\bar{\kappa}_1 - \kappa_2 v$. An element κ of $\mathfrak{C}$ is said to be integral if its norm $\kappa\kappa^*$ and trace $\kappa + \kappa^*$ are in Z. The module of integers consisting of the elements $\kappa_1 + \kappa_2 v$ with κ_1 and κ_2 in L will be denoted by C_0. C_0 is not maximal, but it has a sum of eight squares for its norm-form.

Let $\mathfrak{M}$ be a module of integers in $\mathfrak{C}$ with $k_0, k_1, \ldots, k_7$ as a Z-basis. Since we shall assume $\mathfrak{M}$ contains the identity element, we may take $k_0 = 1$. By the norm-form for the basis $k_0, k_1, \ldots, k_7$ we shall mean the quadratic form

$$N(x) = 1/2 \sum T(k_\alpha \bar{k}_\beta) x_\alpha x_\beta$$

where $x = x_0k_0 + x_1k_1 + \ldots + x_7k_7$. The norm-form will be an integral positive-definite octonary which is rationally equivalent to $\sum_{i=0}^{7} x_i^2$.

Let $f = \sum_{\alpha,\beta=1}^{3} a_{\alpha\beta} x_\alpha x_\beta$ be a ternary quadratic form with matrix $a = (a_{\alpha\beta})$, $a_{\alpha\beta}$ rational, and let $A = (A_{\alpha\beta}) = \text{adj } a$. We shall now define the quaternion algebra associated with the form f. This algebra has four basal elements $1, i_1, i_2, i_3$ satisfying the multiplication table

$$i_\alpha^2 = -A_{\alpha\alpha} \qquad (\alpha = 1, 2, 3)$$

$$i_2 i_3 = -A_{23} + \sum a_{1\alpha} i_\alpha \qquad i_3 i_2 = -A_{32} - \sum a_{1\alpha} i_\alpha$$

with $i_3 i_1$, and so on, obtained by permuting the subscripts cyclically. The elements of the algebra have the form

$$x = x_0 + \sum x_\alpha i_\alpha .$$

The Hamilton quaternions are associated with the form $x_1^2 + x_2^2 + x_3^2$.

In this paper we wish to deal with rings of integral elements. The problem of how to find them naturally arises. One may conjecture that if f has integral coefficients, it should be possible to associate with it in some manner a ring of integral elements. The conjugate $\bar{x}$ of x is $x_0 - x_1 i_1 - x_2 i_2 - x_3 i_3$ and the norm $\bar{x}x = x\bar{x}$ is found to be

$$(1) \quad \psi = x_0^2 + \sum_{\alpha,\beta=1}^{3} A_{\alpha\beta} x_\alpha x_\beta = N(x_0 + x_1 i_1 + x_2 i_2 + x_3 i_3) .$$

When f has integral coefficients, $a_{\alpha\beta}$ can be half an odd

integer if $\alpha \neq \beta$, and hence the coefficients of ψ may not be integral. To obtain in the simplest possible manner a related form which does have integral coefficients, it is natural to try completing squares. Thus:

$$(1') \quad (x_0 + \varepsilon_1/2 \cdot x_1 + \varepsilon_2/2 \cdot x_2 + \varepsilon_3/2 \cdot x_3)^2 + \sum_{\alpha,\beta=1}^{3} A_{\alpha\beta}\, x_\alpha\, x_\beta$$

$$= x_0^2 + \sum \varepsilon_\alpha x_0 x_\alpha + \sum (A_{\alpha\alpha} + \varepsilon_\alpha^2/4)x^2 + (2A_{23} + \varepsilon_2\varepsilon_3/2)x_2x_3$$

$$+ (2A_{31} + \varepsilon_3\varepsilon_1/2)x_3x_1 + (2A_{12} + \varepsilon_1\varepsilon_2/2)x_1x_2 .$$

One finds, fortunately, that ε_1, ε_2, ε_3 can be chosen in Z so that the form in (1') has integral coefficients. In fact, one can and must choose ε_α to be even or odd according as $2a_{\beta\gamma}$ is even or odd where α, β, γ is a permutation of 1, 2, 3. We shall refer to (1') as the Brandt norm-form. Accordingly, with a glance at (1), we naturally consider

$$x_0 + \varepsilon_1/2 \cdot x_1 + \varepsilon_2/2 \cdot x_2 + \varepsilon_3/2 \cdot x_3 + x_1i_1 + x_2i_2 + x_3i_3$$

$$= x_0 + x_1j_1 + x_2j_2 + x_3j_3$$

where $j_\alpha = \varepsilon_\alpha/2 + i_\alpha$ ($\alpha = 1, 2, 3$) and notice that the integral form in (1') is exactly the norm of $x_0 + x_1j_1 + x_2j_2 + x_3j_3$ and can now verify that the system $\{x_0 + x_1j_1 + x_2j_2 + x_3j_3 : x_0, x_1, x_2, x_3 \in Z\}$ is indeed a ring. It is clear that the sum of integral quaternions is integral. Also,

$$j_\alpha^2 = \varepsilon_\alpha j_\alpha - A_{\alpha\alpha} - \varepsilon_\alpha^2/4$$

$$j_2 j_3 = (i_2 + \varepsilon_2/2)(i_3 + \varepsilon_3/2)$$

$$= -A_{23} - 1/2 \sum a_{1\alpha}\varepsilon_\alpha - \varepsilon_2\varepsilon_3/4 + a_{11}j_1$$

$$+ (a_{12} + \varepsilon_3/2)j_2 + (a_{13} + \varepsilon_2/2)j_3 .$$

Now $-A_{\alpha\alpha} - \varepsilon_\alpha^2/4$ is in Z, and likewise

$$A_{23} + 1/2 \sum a_{1\alpha}\varepsilon_\alpha + \varepsilon_2\varepsilon_3/4 = (a_{12} + \varepsilon_3/2)(a_{31} + \varepsilon_2/2)$$

$$- a_{11}(a_{32} + \varepsilon_1/2) + a_{11}\varepsilon_1$$

is in Z. After computing the other products in a similar manner, we see that the system defined above is a ring of integral quaternions.

Let $\mathcal{Q}$ be a quaternion algebra defined as in the previous paragraphs. Let $\mathcal{M}$ be a module of integers in $\mathcal{Q}$ with a Z-basis k_0, k_1, k_2, k_3. Since we shall assume that $\mathcal{M}$ contains the identity element, we may take $k_0 = 1$. $\mathcal{M}$ has $h^2 + g$ for its norm-form where

$$h = 1/2 \sum T(k_\alpha)x_\alpha$$

$$g = 1/4 \sum \left(T(k_\alpha \bar{k}_\beta) - T(k_\alpha k_\beta) \right) x_\alpha x_\beta .$$

Pall and Irwin have characterized the modules which are rings in terms of their norm-forms. In [3][1] Irwin shows

---

[1]Pairs of Arabic numerals in brackets refer to correspondingly numbered references in the Selected Bibliography and page numbers, respectively. A single Arabic numeral in a bracket refers to the correspondingly numbered reference in the Selected Bibliography.

that there exists a ternary form f with rational coefficients, unique except for sign, such that g = adj f. $\mathcal{M}$ is then a ring if and only if the coefficients of f are in Z. Also, results of [3] show that every maximal module of integers in $\mathcal{H}$ is also a ring.

In the Cayley algebra it is not true that maximal modules of integers are necessarily rings. However, Estes and Pall have shown in a forthcoming paper [2] that a maximal module of integers which contains the naive ring C_0 possesses an isomorphic module which is a ring.

It is now natural to ask if a module of integers in $\mathcal{C}$ which is a ring can be characterized in some way by its norm-form. In this paper we shall consider modules of integers over the local ring Z/p^r, p a prime. We show that a module of integers with any of certain types of norm-forms is a ring. Also, conditions on the norm-form are obtained in order that a module of integers possess an isomorph (in the module sense) which is a ring.

Van der Blij and Springer in [7] show that a module $\mathcal{M}$ of integers in $\mathcal{C}$ is a maximal ring if and only if (1) the identity e is in $\mathcal{M}$, (2) $(xy,z) \in Z$ if $x, y, z \in \mathcal{M}$, where $(a,b) = N(a + b) - N(a) - N(b)$ is a bilinear function, (3) $\mathcal{M}$ is a maximal module on which $N(x) \in Z$.

CHAPTER I

NOTATION; BASIC PROPERTIES

In this paper we shall denote by $F(p)$ the field of p-adic numbers and by $F(\infty)$ the field of real numbers.

We shall use the notation (a/p) for the Legendre symbol recalling that $(a/p) = +1$ if $a \not\equiv 0 \bmod p$ and a is a quadratic residue mod p, and $(a/p) = -1$ if a is a quadratic non-residue mod p.

If p is any prime, and a and b are non-zero rationals, the Hilbert symbol $(a,b)_p$ will be defined to be $+1$ if there exist x_1, x_2 in $F(p)$ such that $ax_1^2 + bx_2^2 = 1$, and -1 otherwise. If we write $a = p^u a'$ and $b = p^v b'$ with a' and b' prime to p, we have the following formulas for the evaluation of $(a,b)_p$:

$(p^u a', p^v b')_p = (a'/p)^v (b'/p)^u (-1/p)^{uv}$, if p is odd;

$(2^u a', 2^v b')_2 = (2/a')^v (2/b')^u (-1)^k$, where $k = (a'-1)(b'-1)/4$,

and where $(2/m)$ denotes $+1$ if $m \equiv \pm 1 \bmod 8$, -1 if $m \equiv \pm 3 \bmod 8$. All this can be interpreted for p-adic numbers instead of rational numbers in the obvious way.

Let f be a quadratic form with coefficients in $F(p)$ and non-zero determinant. If A is the matrix of f, by D_i we shall mean the leading i by i determinant in the upper

left hand corner of A. If [cf.(6)] f has no two successive $D_i = 0$, we shall define the Hasse symbol $c_p(f)$ as follows:

$$c_p(f) = (-1, -D_n)_p \prod_{i=1}^{n-1} (D_i, -D_{i+1})_p .$$

In this paper we shall make use of the following theorem:

Theorem: Two forms with rational coefficients and non-zero determinants d_1 and d_2 and n_1 and n_2 variables respectively are rationally equivalent if and only if $n_1 = n_2$, $d_1 = t^2 d_2$, and they are p-adically equivalent for every p. The conditions of p-adic equivalence when p is a finite prime are (if $n_1 = n_2$ and d_1/d_2 is a p-adic square) $c_p(f_1) = c_p(f_2)$, and for the prime ∞ it is that the forms have the same index (the invariant under real non-singular transformations).

If the transformation $x_i = \sum_{j=1}^{s} t_{ij} y_j$, $t_{ij} \in Z$, $(i = 1, \ldots, s)$ with matrix $T = (t_{ij})$ carries the integral form $f(x_1, \ldots, x_s)$ into the integral form $g(y_1, \ldots, y_s) = \sum b_{ij} y_i y_j$, $(i,j = 1, \ldots, s)$ then $B = T'AT$ where T' denotes the transpose of T, B represents the matrix of g, and A represents the matrix of f. If $|T|$, the determinant of T, is 1, then T^{-1} is a matrix with elements in Z, and we can write $A = (T^{-1})'BT$. If f is transformable into g by a transformation of determinant 1, we shall call f and g unimodularly equivalent or, briefly, equivalent. All

forms equivalent to a given form are equivalent to each other and constitute a class of forms.

Two forms f and g will be called equivalent, to the modulus N, if there exists in the class of f a form whose coefficients are congruent, to the modulus N, to the corresponding coefficients of g. In [5;35] Pall, essentially following Minkowski, gives the following two lemmas:

Lemma: Let $s \geq 2$, $f = \sum_{i,j=1}^{s} a_{ij}x_i x_j$. Let t be positive, p an odd prime. Then f is equivalent, to the modulus p^t, to a form g of the type

$$g(y_1, \ldots, y_s) = p^{\alpha_1} m_1 y_1^2 + p^{\alpha_2} m_2 y_2^2 + \ldots + p^{\alpha_s} m_s y_s^2$$
$$(0 \leq \alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_s),$$

the α_i being integers and the m_i prime to p.

Lemma: Let $s \geq 2$, $t > 0$. Then f is equivalent, to the modulus 2^t, to a form of the type

$$g(y_1, \ldots, y_s) = 2^{\beta_1} m_1 y_1^2 + \ldots + 2^{\beta_u} m_u y_u^2$$
$$+ 2^{\gamma_1}(n_1 y_{u+1}^2 + m^{(1)} y_{u+1}y_{u+2} + n_2 y_{u+2}^2)$$
$$+ \ldots + 2^{\gamma_v}(n_{2v-1} y_{s-1}^2 + m^{(v)} y_{s-1}y_s + n_{2v} y_s^2),$$

where (a) the β_i and γ_j are non-negative integers, the $m^{(j)}$ are odd, and $s = u + 2v$, $u \geq 0$, $v \geq 0$;

(b) the $m^{(j)}$ may be taken to be arbitrary odd

integers, and $n_1, n_3, \ldots, n_{2v-1}$ to be odd;

(c) for no i and j is $a\beta_i + 1$ equal to a γ_j.

Let $\mathfrak{M}$ be a module of integers in $\mathfrak{L}$ with $j_0, j_1, \ldots, j_7$ as a Z-basis and norm-form f. Let j denote the row vector $(j_0, j_1, \ldots, j_7)$. Consider a transformation with matrix $T = (t_{ij})$, $t_{ij} \in Z$, $|T| = 1$, and let T carry f into some form g. Then $\mathfrak{M}$ is transformed into an isomorphic module $\mathfrak{M}'$ of integers with norm-form g. Also, $k = (k_0, k_1, \ldots, k_7) = j \cdot T$, and $k_0, k_1, \ldots, k_7$ is a Z-basis of $\mathfrak{M}'$. Hence we see that every module of integers $\mathfrak{M}$ possesses an isomorph $\mathfrak{M}'$ whose norm-form has a residue modulo p^t given by one of the lemmas in the preceding paragraph.

Let $f = \sum_{i,j=1}^{s} a_{ij} x_i x_j$ be an integral form with matrix A. By d_k we shall denote the g.c.d. of the set of principal minor determinants of order k in A and the doubles of the non-principal minors of order k. We shall define

$$o_k = \frac{4 d_{k-1} d_{k+1}}{d_k^2} \qquad (k = 1, \ldots, s-1)$$

$$o_0 = o_n = 0 .$$

Pall has shown in [5;33] the following properties of the o_k:

The o_k are integers; moreover, $o_1, \ldots, o_{s-1}$ are positive

$o_k \not\equiv 2 \bmod 4 \quad (k = 0, 1, \ldots, s)$

If any o_k $(k = 1, \ldots, s-1)$ is odd, then $o_{k-1} \equiv o_{k+1} \equiv 0 \bmod 16$

$o_k(tf) = o_k(f)$ for t a real number.

All forms in s variables with the same index, the same divisor d_1, and the same value of the invariants $o_1, \ldots, o_{s-1}$ constitute an order. The $o_1, \ldots, o_{s-1}$ are called the o-invariants.

CHAPTER II

MODULES WHICH ARE RINGS

In this chapter we shall consider modules of integers over the local ring Z/p^r, p a prime, and show that modules with certain norm-forms are rings.

We first consider the case of odd primes. In view of the lemma of the previous chapter, an integral ternary form is equivalent, to the modulus p^t, to a form of the type $p^{a_1}m_1x_1^2 + p^{a_2}m_2x_2^2 + p^{a_3}m_3x_3^2$ where $0 \leq a_1 \leq a_2 \leq a_3$ and m_i is prime to p for i = 1, 2, 3. Thus, an integral ternary form with coefficients in Z/p^r is equivalent to a diagonal form of the type just mentioned.

Theorem 1: Let p be an odd prime and $f = p^{a_1}m_1x_1^2 + \ldots + p^{a_3}m_3x_3^2$ where $0 \leq a_1 \leq \ldots \leq a_3$ and m_i prime to p for i = 1, 2, 3. The module $\mathcal{M}$ whose norm-form is F + cF where $F = x_0^2 + \text{adj } f$ is a ring if and only if c is integral.

Proof: We denote the matrix of f by $a = \begin{bmatrix} p^{a_1}m_1 & 0 & 0 \\ 0 & p^{a_2}m_2 & 0 \\ 0 & 0 & p^{a_3}m_3 \end{bmatrix}$ and the matrix of adj f by

$A = \begin{bmatrix} p^{a_2+a_3}m_2m_3 & 0 & 0 \\ 0 & p^{a_1+a_3}m_1m_3 & 0 \\ 0 & 0 & p^{a_1+a_2}m_1m_2 \end{bmatrix}$. The quaternion algebra associated with f has four basal elements 1, j_1, j_2, j_3 which satisfy the multiplication table

$$j_1^2 = -p^{a_2+a_3}m_2m_3, \quad j_2^2 = -p^{a_1+a_3}m_1m_3, \quad j_3^2 = -p^{a_1+a_2}m_1m_2$$

(2) $j_1j_2 = p^{a_3}m_3j_3, \quad j_1j_3 = -p^{a_2}m_2j_2, \quad j_2j_3 = p^{a_1}m_1j_1$

and $j_rj_s = -j_sj_r$ for r,s = 1, 2, 3.

$\mathcal{M}$ has for a Z-basis the eight elements 1, j_1, j_2, j_3, j_4, j_5, j_6, j_7 where

(3) $j_4^2 = -c, \quad j_5 = j_1j_4, \quad j_6 = j_2j_4, \quad j_7 = j_3j_4$.

Since $j_4^2 = -c$, c must be integral. In view of (2) and (3) we have closure for all products j_rj_s, r,s = 1, 2, ... ,7 if and only if c is integral.

We now consider the prime 2. Pall has shown in [4;299] that an integral ternary form is equivalent, to the modulus 2^t, to one of the three following types of forms:

i) $2^{a_1}m_1x_1^2 + 2^{a_2}m_2x_2^2 + 2^{a_3}m_3x_3^2$, $0 \leq a_1 \leq a_2 \leq a_3$, m_i odd,

ii) $2^{\beta+2}(jx_1^2 + x_1x_2 + jx_2^2) + 2^{\alpha}mx_3^2$, $\beta \geq 0$, $0 \leq \alpha \leq \beta$, $j = 0$ or 1,

iii) $2^{\delta}(jx_1^2 + x_1x_2 + jx_2^2 + \lambda x_3^2)$, $\delta \geq 0$, λ even if $j = 1$.

Hence, an integral ternary form with coefficients in $Z/2^r$ is equivalent to one of the three types of forms mentioned above.

Again, let $F = x_0^2 + \text{adj } f$ where f is the form in i), ii), or iii). Now let c be in Q and consider the form $F + cF$. When $F + cF$ is not an integral form, it may be possible for some values of c to choose a matrix $V^{(4,4)}$ with elements 0 or 1 such that the transformation T whose matrix is $\begin{bmatrix} I_4 & 1/2 \cdot V \\ 0 & I_4 \end{bmatrix}$ carries $F + cF$ into an integral form which we shall denote by $\mathcal{F}$.

$$\begin{bmatrix} F_* & 1/2 \cdot F_* V \\ 1/2 \cdot V' F_* & 1/4 \cdot V' F_* V + cF_* \end{bmatrix} =$$

$$\begin{bmatrix} I_4 & 0 \\ 1/2 \cdot V' & I_4 \end{bmatrix} \begin{bmatrix} F_* & 0 \\ 0 & cF_* \end{bmatrix} \begin{bmatrix} I_4 & 1/2 \cdot V \\ 0 & I_4 \end{bmatrix},$$

with F_* denoting the matrix of F, is the matrix of an integral form if $1/4 \cdot V' F_* V + cF_*$ is the matrix of an integral form (or $1/4 \cdot V' F_* V + cF_*$ is semi-integral).

In i) F_* is of the type $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & x & 0 & 0 \\ 0 & 0 & y & 0 \\ 0 & 0 & 0 & z \end{bmatrix}$ and of the type $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & x & y & 0 \\ 0 & y & x & 0 \\ 0 & 0 & 0 & z \end{bmatrix}$ in ii) and iii). V will be denoted by (v_{ij}), $0 \leq i, j \leq 3$, with $v_{ij} = 0$ or 1.

We can now state the following results:

Theorem 2: Let f be of type i). Then $\mathcal{F}$ is an integral form if and only if one of conditions a), b), or c) holds.

a) c is in Z.

b) $c = k/2$ with k odd, $a_1 = 0$, and $a_2 = 1$.

c) $c = k/4$ with $k \equiv 3 \bmod 4$, or $k \equiv 1 \bmod 4$ and

$$\begin{cases} a_1, a_2, a_3 = 0 \\ a_1, a_2 = 0,\ a_3 \geq 1,\ m_1 m_2 \equiv 3 \bmod 4 \\ a_1, a_2 = 0,\ a_3 = 1,\ m_1 m_2 \equiv 1 \bmod 4 \\ a_1 = 0,\ a_2 = 1,\ a_3 \geq 1. \end{cases}$$

Theorem 3: Let f be of type ii). Then $\mathcal{F}$ is an integral form if and only if one of the conditions a) or b) holds.

a) c is in Z.

b) $c = k/4$ with $k \equiv 3 \bmod 4$.

Theorem 4: Let f be of type iii). Then $\mathcal{F}$ is an integral form if and only if one of conditions a) or b) holds.

a) c is in Z.

b) $c = k/4$ with $k \equiv 3 \bmod 4$, $\delta > 0$, or
$k \equiv 1 \bmod 4$, $\delta = 1$, and
$\lambda \equiv 0 \bmod 8$.

Proof of Theorem 2: We have $x = 2^{a_2+a_3} m_2 m_3$, $y = 2^{a_1+a_3} m_1 m_3$, $z = 2^{a_1+a_2} m_1 m_2$ for the entries in F_*. The matrix $1/4 \cdot V' F_* V + cF_*$ is symmetric, and we shall denote it by (b_{ij}), $0 \leq i,j \leq 3$ with $b_{ij} = b_{ji}$ for $i \neq j$. We have that

$$b_{00} = 1/4\,(v_{00}^2 + xv_{10}^2 + yv_{20}^2 + zv_{30}^2) + c$$
$$b_{11} = 1/4\,(v_{01}^2 + xv_{11}^2 + yv_{21}^2 + zv_{31}^2) + cx$$
$$b_{22} = 1/4\,(v_{02}^2 + xv_{12}^2 + yv_{22}^2 + zv_{32}^2) + cy$$
$$b_{33} = 1/4\,(v_{03}^2 + xv_{13}^2 + yv_{23}^2 + zv_{33}^2) + cz$$

$$b_{10} = 1/4\,(v_{00}v_{01} + xv_{10}v_{11} + yv_{20}v_{21} + zv_{30}v_{31})$$
$$b_{20} = 1/4\,(v_{00}v_{02} + xv_{10}v_{12} + yv_{20}v_{22} + zv_{30}v_{32})$$
$$b_{30} = 1/4\,(v_{00}v_{03} + xv_{10}v_{13} + yv_{20}v_{23} + zv_{30}v_{33})$$

$$b_{21} = 1/4\,(v_{01}v_{02} + xv_{11}v_{12} + yv_{21}v_{22} + zv_{31}v_{32})$$
$$b_{31} = 1/4\,(v_{01}v_{03} + xv_{11}v_{13} + yv_{21}v_{23} + zv_{31}v_{33})$$

$$b_{32} = 1/4\,(v_{02}v_{03} + xv_{12}v_{13} + yv_{22}v_{23} + zv_{32}v_{33}).$$

If (b_{ij}) is the matrix of an integral form, then the b_{ij}, $i = j$, must be integers and the b_{ij}, $i \neq j$, must be halves of integers. That is, we must have

$$v_{00}^2 + 2^{a_2+a_3} m_2 m_3 v_{10}^2 + 2^{a_1+a_3} m_1 m_3 v_{20}^2 + 2^{a_1+a_2} m_1 m_2 v_{30}^2 + 4c \equiv 0 \bmod 4$$

$$v_{01}^2 + 2^{a_2+a_3} m_2 m_3 (v_{11}^2 + 4c) + 2^{a_1+a_3} m_1 m_3 v_{21}^2 + 2^{a_1+a_2} m_1 m_2 v_{31}^2 \equiv 0 \bmod 4$$

$$v_{02}^2 + 2^{a_2+a_3} m_2 m_3 v_{12}^2 + 2^{a_1+a_3} m_1 m_3 (v_{22}^2 + 4c) + 2^{a_1+a_2} m_1 m_2 v_{32}^2 \equiv 0 \bmod 4$$

$$v_{03}^2 + 2^{a_2+a_3} m_2 m_3 v_{13}^2 + 2^{a_1+a_3} m_1 m_3 v_{23}^2 + 2^{a_1+a_2} m_1 m_2 (v_{33}^2 + 4c) \equiv 0 \bmod 4,$$

$$v_{00}v_{0r} + 2^{a_2+a_3} m_2 m_3 v_{10}v_{1r} + 2^{a_1+a_3} m_1 m_3 v_{20}v_{2r} + 2^{a_1+a_2} m_1 m_2 v_{30}v_{3r} \equiv 0 \bmod 2 \text{ for } r = 1, 2, 3,$$

$$v_{01}v_{0r} + 2^{a_2+a_3} m_2 m_3 v_{11}v_{1r} + 2^{a_1+a_3} m_1 m_3 v_{21}v_{2r} + 2^{a_1+a_2} m_1 m_2 v_{31}v_{3r} \equiv 0 \bmod 2 \text{ for } r = 2, 3, \text{ and}$$

$$v_{02}v_{03} + 2^{a_2+a_3} m_2 m_3 v_{12}v_{13} + 2^{a_1+a_3} m_1 m_3 v_{22}v_{23} + 2^{a_1+a_2} m_1 m_2 v_{32}v_{33} \equiv 0 \bmod 2.$$

We first show that if one of conditions a), b), or c) does not hold, then (b_{ij}) is not the matrix of an integral form.

First, suppose $c = k/8$ with k odd. If b_{00} is to be integral we must have

$$2v_{00}^2 + 2^{\alpha_2+\alpha_3+1} m_2 m_3 v_{10}^2 + 2^{\alpha_1+\alpha_3+1} m_1 m_3 v_{20}^2 + 2^{\alpha_1+\alpha_2+1} m_1 m_2 v_{30}^2 + k \equiv 0 \bmod 8$$

which is impossible with k odd.

Next, suppose $c = k/4$ with $k \equiv 1 \bmod 4$ and $\alpha_1 > 0$. If b_{00} is to be integral, we must have $v_{00}^2 + k \equiv 0 \bmod 4$ which is impossible with $v_{00} = 0$ or 1 and $k \equiv 1 \bmod 4$. Now, if $\alpha_1 = 0$ and $\alpha_2 > 1$, we must have $v_{00}^2 + k \equiv 0 \bmod 4$ which is again impossible. In the case of $\alpha_1 = \alpha_2 = 0, \alpha_3 > 1$, $m_1 m_2 \equiv 1 \bmod 4$, we have $v_{00}^2 + m_1 m_2 v_{00}^2 + k \equiv 0 \bmod 4$, and therefore b_{00} cannot be integral.

Finally, suppose $c = k/2$ with k odd. If $\alpha_1 > 0$, we must have $v_{00}^2 + 2k \equiv 0 \bmod 4$ if b_{00} is to be integral. This is clearly impossible with k odd. Next, if $\alpha_1 = 0$ and $\alpha_2 > 1$, we have the same impossible condition.

We now show that any one of conditions a), b), or c) gives rise to a semi-integral matrix (b_{ij}).

For condition c) if $k \equiv 3 \bmod 4$ and we take

$V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, it is clear that (b_{ij}) is semi-integral. For $k \equiv 1 \bmod 4$ and $a_3 = 0$, we take

$V = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$. For $a_1 = 0, a_2 = 1, a_3 = 1$ we may take $V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ v_{10} & v_{11} & v_{12} & v_{13} \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$ or $\begin{bmatrix} 1 & 0 & 0 & 0 \\ v_{10} & v_{11} & v_{12} & v_{13} \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$ with $v_{10}, v_{11}, v_{12}, v_{13}$ arbitrarily 0 or 1. If $a_1 = 0$, $a_2 = 1$, $a_3 > 1$, we may take

$V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ v_{10} & v_{11} & 1 & v_{13} \\ v_{20} & 1 & v_{22} & v_{23} \\ 1 & 0 & 0 & 1 \end{bmatrix}$ with $v_{10}, v_{11}, v_{13}, v_{20}, v_{22}$, and v_{23} arbitrarily 0 or 1. For $a_1 = a_2 = 0$, we may take $V = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$ if $a_3 \geq 1$, $m_1 m_2 \equiv 3 \bmod 4$,

and $V = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$ if $\alpha_3 = 1$, $m_1 m_2 \equiv 1 \bmod 4$.

For condition b) we have that $c = k/2$, k odd, $\alpha_1 = 0$ and $\alpha_2 = 1$. We may take

$V = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$ and get (b_{ij}) semi-integral.

For condition a) we take $V = (0)$.

In the proof of Theorems 3 and 4, the elements of the matrix (b_{ij}) are the following:

$$b_{00} = 1/4\,[v_{00}^2 + x(v_{10}^2 + v_{20}^2) + 2yv_{10}v_{20} + zv_{30}^2] + c$$

$$b_{11} = 1/4\,[v_{01}^2 + x(v_{11}^2 + v_{21}^2) + 2yv_{11}v_{21} + zv_{31}^2] + cx$$

$$b_{22} = 1/4\,[v_{02}^2 + x(v_{12}^2 + v_{22}^2) + 2yv_{12}v_{22} + zv_{32}^2] + cx$$

$$b_{33} = 1/4\,[v_{03}^2 + x(v_{13}^2 + v_{23}^2) + 2yv_{13}v_{23} + zv_{33}^2] + cx$$

$$b_{10} = 1/4\,[v_{00}v_{01} + x(v_{10}v_{11} + v_{20}v_{21}) + y(v_{10}v_{21} + v_{20}v_{11}) + zv_{30}v_{31}]$$

$$b_{20} = 1/4\,[v_{00}v_{02} + x(v_{10}v_{12} + v_{20}v_{22}) + y(v_{10}v_{22} + v_{20}v_{21}) + zv_{30}v_{32}]$$

$$b_{30} = 1/4\,[v_{00}v_{03} + x(v_{10}v_{13} + v_{20}v_{23}) + y(v_{10}v_{23} + v_{20}v_{23}) + zv_{30}v_{33}]$$

$$b_{21} = 1/4\,[v_{01}v_{02} + x(v_{11}v_{12} + v_{21}v_{22}) + y(v_{11}v_{22} + v_{12}v_{21}) + zv_{31}v_{32}] + cy$$

$$b_{31} = 1/4\,[v_{01}v_{03} + x(v_{11}v_{13} + v_{21}v_{23}) + y(v_{11}v_{23} + v_{21}v_{13}) + zv_{31}v_{33}]$$

$$b_{32} = 1/4\,[v_{02}v_{03} + x(v_{02}v_{13} + v_{22}v_{23}) + y(v_{02}v_{23} + v_{12}v_{13}) + zv_{32}v_{33}]$$

Proof of Theorem 3: For the entries of F_*, we have $x = 2^{\alpha+\beta+2}mj$, $y = -2^{\alpha+\beta+1}m$, and $z = 2^{2(\beta+1)}(4j^2 - 1)$ with $\beta \geq 0$, $0 \leq \alpha \leq \beta$, and $j = 0$ or 1.

Again, if (b_{ij}) is to be a matrix of an integral form we must have

$$v_{00}^2 + 2^{\alpha+\beta+2}mj(v_{10}^2 + v_{20}^2) - 2^{\alpha+\beta+2}mv_{10}v_{20} + 2^{2(\beta+1)}(4j^2 - 1)v_{30}^2 + 4c \equiv 0 \bmod 4,$$

$$v_{01}^2 + 2^{\alpha+\beta+2}mj(v_{11}^2 + v_{21}^2) - 2^{\alpha+\beta+2}mv_{11}v_{21}$$
$$+ 2^{2(\beta+1)}(4j^2 - 1)v_{31}^2 + 2^{\alpha+\beta+4}mjc \equiv 0 \bmod 4,$$

$$v_{02}^2 + 2^{\alpha+\beta+2}mj(v_{12}^2 + v_{22}^2) - 2^{\alpha+\beta+2}mv_{12}v_{22}$$
$$+ 2^{2(\beta+1)}(4j^2 - 1)v_{32}^2 + 2^{\alpha+\beta+4}mjc \equiv 0 \bmod 4,$$

$$v_{03}^2 + 2^{\alpha+\beta+2}mj(v_{13}^2 + v_{23}^2) - 2^{\alpha+\beta+2}mv_{13}v_{23}$$
$$+ 2^{2(\beta+1)}(4j^2 - 1)\, v_{33}^2 + 2^{2(\beta+2)}(4j^2 - 1)c \equiv 0 \bmod 4,$$

$$v_{00}v_{0r} + 2^{\alpha+\beta+2}mj(v_{10}v_{1r} + v_{20}v_{2r}) - 2^{\alpha+\beta+1}m(v_{10}v_{2r} + v_{20}v_{1r})$$
$$+ 2^{2(\beta+1)}(4j^2 - 1)v_{30}v_{3r} \equiv 0 \bmod 2, \text{ for } r = 1, 2, 3,$$

$$v_{01}v_{02} + 2^{\alpha+\beta+2}mj(v_{11}v_{12} + v_{21}v_{22}) - 2^{\alpha+\beta+1}m(v_{11}v_{22} + v_{12}v_{21})$$
$$+ 2^{2(\beta+1)}(4j^2 - 1)v_{31}v_{32} - 2^{\alpha+\beta+3}mc \equiv 0 \bmod 2,$$

$$v_{01}v_{03} + 2^{\alpha+\beta+2}mj(v_{11}v_{13} + v_{21}v_{23}) - 2^{\alpha+\beta+1}m(v_{11}v_{23} + v_{21}v_{13})$$
$$+ 2^{2(\beta+1)}(4j^2 - 1)v_{31}v_{33} \equiv 0 \bmod 2,$$

$$v_{02}v_{03} + 2^{\alpha+\beta+2}mj(v_{02}v_{13} + v_{22}v_{23}) - 2^{\alpha+\beta+1}m(v_{02}v_{23} + v_{12}v_{13})$$
$$+ 2^{2(\beta+1)}(4j^2 - 1)v_{32}v_{33} \equiv 0 \bmod 2.$$

We first show that if either condition a) or b) does not hold, then (b_{ij}) is not semi-integral.

Suppose that $c = k/8$ with k odd. If b_{00} is to be integral we must have $2v_{00}^2 + k \equiv 0 \bmod 8$, which is impossible.

Next, suppose that $c = k/4$ with $k \equiv 1 \bmod 4$. We must have $v_{00}^2 + k \equiv 0 \bmod 4$ if b_{00} is to be integral, but this is impossible with $k \equiv 1 \bmod 4$ and $v_{00} = 0$ or 1.

Finally, suppose that $c = k/2$ with k odd. It must be true that $v_{00}^2 + 2k \equiv 0 \bmod 4$ for b_{00} to be integral. This is again impossible with k odd and $v_{00} = 0$ or 1.

We now show that either condition a) or b) gives rise to a semi-integral matrix (b_{ij}).

For condition b) we have that $c = k/4$ with $k \equiv 3 \bmod 4$. If we take $V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, it is clear that (b_{ij}) is semi-integral.

For condition a) we have that c is in Z. We can then take $V = (0)$ since cF_* is an integral matrix.

Proof of Theorem 4: Here we have $x = 2^{2\delta}\lambda j$, $y = -2^{2\delta-1}\lambda$, $z = 2^{2(\delta-1)}(4j^2 - 1)$ with $\delta \geq 0$, $j = 0$ or 1, and λ even if $j = 1$ for the entries of F_*. We first consider the case $\delta > 0$. That is, f is an integral form.

If (b_{ij}) is to be a semi-integral matrix, we must have

$$v_{00}^2 + 2^{2\delta}\lambda j(v_{10}^2 + v_{20}^2) - 2^{2\delta}\lambda v_{10}v_{20} + 2^{2(\delta-1)}(4j^2 - 1)v_{30}^2 + 4c \equiv 0 \bmod 4,$$

$$v_{01}^2 + 2^{2\delta}\lambda j(v_{11}^2 + v_{21}^2) - 2^{2\delta}\lambda v_{11}v_{21} + 2^{2(\delta-1)}(4j^2 - 1)v_{31}^2 + 2^{2\delta+2}\lambda jc \equiv 0 \bmod 4,$$

$$v_{02}^2 + 2^{2\delta}\lambda j(v_{12}^2 + v_{22}^2) - 2^{2\delta}\lambda v_{12}v_{22} + 2^{2(\delta-1)}(4j^2 - 1) + 2^{2\delta+2}\lambda jc \equiv 0 \bmod 4,$$

$$v_{03}^2 + 2^{2\delta}\lambda j(v_{13}^2 + v_{23}^2) - 2^{2\delta}\lambda v_{13}v_{23} + 2^{2(\delta-1)}(4j^2 - 1) + 2^{2\delta}(4j^2 - 1)c \equiv 0 \bmod 4,$$

$$v_{00}v_{0r} + 2^{2\delta}\lambda j(v_{10}v_{1r} + v_{20}v_{2r}) - 2^{2\delta-1}\lambda(v_{10}v_{2r} + v_{20}v_{1r}) + 2^{2(\delta-1)}(4j^2 - 1)v_{30}v_{3r} \equiv 0 \bmod 2, \text{ for } r = 1, 2, 3,$$

$$v_{01}v_{02} + 2^{2\delta}\lambda j(v_{11}v_{12} + v_{21}v_{22}) - 2^{2\delta-1}\lambda(v_{11}v_{22} + v_{12}v_{21}) + 2^{2(\delta-1)}(4j^2 - 1)v_{31}v_{32} - 2^{2\delta-1}\lambda c \equiv 0 \bmod 2,$$

$$v_{01}v_{03} + 2^{2\delta}\lambda j(v_{11}v_{13} + v_{21}v_{23}) - 2^{2\delta-1}\lambda(v_{11}v_{23} + v_{21}v_{13}) + 2^{2(\delta-1)}(4j^2 - 1)v_{31}v_{33} \equiv 0 \bmod 2,$$

$$v_{02}v_{03} + 2^{2\delta}\lambda j(v_{02}v_{13} + v_{22}v_{23}) - 2^{2\delta-1}\lambda(v_{02}v_{23} + v_{12}v_{13}) + 2^{2(\delta-1)}(4j^2 - 1)v_{32}v_{33} \equiv 0 \bmod 2.$$

We first show that (b_{ij}) cannot be semi-integral if either condition a) or b) does not hold.

Suppose $c = k/8$ with k odd. We must have

$$2v_{00}^2 + 2^{\gamma}(4j^2 - 1)v_{30}^2 + k \equiv 0 \bmod 8, \quad \gamma > 0$$

which is impossible with k odd.

Suppose $c = k/2$ with k odd. The condition

$$v_{00}^2 + 2^{2(\delta-1)}(4j^2 - 1)v_{30}^2 + 2k \equiv 0 \bmod 4$$

cannot possibly be satisfied.

Next, suppose $c = k/4$ with $k \equiv 1 \bmod 4$. If $\delta > 1$, we must have $v_{00}^2 + k \equiv 0 \bmod 4$ for b_{00} to be integral. This is impossible with $k \equiv 1 \bmod 4$ and $v_{00} = 0$ or 1. In the case $\delta = 1$, b_{21} cannot be semi-integral if λ is odd. Now suppose $\lambda \not\equiv 0 \bmod 8$. The integrality condition for b_{21} is $v_{01}v_{02} + (4j^2 - 1)v_{31}v_{32} - \ell k \equiv 0 \bmod 4$ where $\lambda = 2\ell$. If $\lambda \equiv 2 \bmod 4$, we contradict the integrality of b_{11} and b_{22}. If $\lambda \equiv 0 \bmod 4$ and $\lambda \not\equiv 0 \bmod 8$, we cannot have b_{21} semi-integral.

In the case $\delta = 0$, f is not an integral form, and hence $F = x_0^2 + \operatorname{adj} f$ is not an integral form. However, it is possible to apply a translation to F and obtain an integral form G. We have

$F_0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \lambda j & -\lambda/2 & 0 \\ 0 & -\lambda/2 & \lambda j & 0 \\ 0 & 0 & 0 & j^2-1/4 \end{bmatrix}$. Applying to F_0 the

translation matrix $T = \begin{bmatrix} 1 & 0 & 0 & 1/2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, we obtain

$G_* = T'F_*T = \begin{bmatrix} 1 & 0 & 0 & 1/2 \\ 0 & \lambda_j & -\lambda_j/2 & 0 \\ 0 & -\lambda_j/2 & \lambda_j & 0 \\ 1/2 & 0 & 0 & j^2 \end{bmatrix}$ which is the matrix of an integral form. We now consider the form $G + cG$ with c in Q and show that unless c is in Z it is not possible to choose a matrix $V^{(4,4)}$ with elements 0 or 1 such that the transformation whose matrix is $\begin{bmatrix} I_4 & 1/2 \cdot V \\ 0 & I_4 \end{bmatrix}$ carries $G + cG$ into an integral form.

Again

$$\begin{bmatrix} I_4 & 0 \\ 1/2 \cdot V' & I_4 \end{bmatrix} \begin{bmatrix} G_* & 0 \\ 0 & cG_* \end{bmatrix} \begin{bmatrix} I_4 & 1/2 \cdot V \\ 0 & I_4 \end{bmatrix}$$

$$= \begin{bmatrix} G_* & 1/2 \cdot G_* V \\ 1/2 \cdot V' G_* & 1/4 \cdot V' G_* V + cG_* \end{bmatrix}$$

Here $(b_{ij}) = 1/4 \cdot V'G_*V + cG_*$ must be semi-integral, and $1/2 \cdot V'G_*$, $1/2 \cdot G_*V$ must have elements with denominators at most 2. Now

$$1/2\ V'G_* = 1/2 \begin{bmatrix} v_{00} & v_{10} & v_{20} & v_{30} \\ v_{01} & v_{11} & v_{21} & v_{31} \\ v_{02} & v_{12} & v_{22} & v_{32} \\ v_{03} & v_{13} & v_{23} & v_{33} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 1/2 \\ 0 & \lambda j & -\lambda/2 & 0 \\ 0 & -\lambda/2 & \lambda j & 0 \\ 1/2 & 0 & 0 & j^2 \end{bmatrix}$$

Therefore, $v_{30}, v_{31}, v_{32}, v_{33}, v_{00}, v_{01}, v_{02}, v_{03} = 0$. If λ is odd, $V = (0)$. If $j = 0$, λ must be even or $V = (0)$.

In order that (b_{ij}) be semi-integral, the diagonal elements must be integral. That is,

$$v_{00}^2 + (v_{10}^2 + v_{20}^2)\lambda j + v_{30}^2 j^2 + v_{00}v_{30} - \lambda v_{10}v_{20} + 4c \equiv 0 \bmod 4,$$

$$v_{01}^2 + (v_{11}^2 + v_{21}^2 + 4c)\lambda j + v_{31}v_{01} - \lambda v_{11}v_{21} + v_{31}^2 j^2 \equiv 0 \bmod 4,$$

$$v_{02}^2 + (v_{12}^2 + v_{22}^2 + 4c)\lambda j + v_{32}v_{02} - \lambda v_{12}v_{22} + v_{32}^2 j^2 \equiv 0 \bmod 4,$$

$$v_{03}^2 + (v_{13}^2 + v_{23}^2)\lambda j + (v_{33}^2 + 4c)j^2 + v_{03}v_{33} - \lambda v_{13}v_{23} \equiv 0 \bmod 4.$$

The non-diagonal elements must be at worst halves of integers. The condition for semi-integrality of b_{03} is that

$$2v_{00}v_{03} + v_{30}v_{03} + 2v_{10}v_{13}\lambda j - v_{20}v_{13}\lambda + 2v_{20}v_{23}\lambda j - v_{10}v_{23}\lambda + 2v_{30}v_{33}j^2 + v_{00}v_{33} + c$$

be an integer.

Suppose $c = k/2$ with k odd. If $j = 1$, λ is even. If $\lambda \equiv 0 \bmod 4$, b_{00} cannot possibly be integral. If $\lambda \equiv 2 \bmod 4$, we must have $v_{10}, v_{20}, v_{13}, v_{23} = 1$ which contradicts the semi-integrality of b_{03}. If $j = 0$, λ still must be even. We have the same situation as before if $\lambda \equiv 0 \bmod 4$. If $\lambda \equiv 2 \bmod 4$ we must have $v_{10}, v_{20} = 1$ and one of v_{13} or v_{23} equal to 0. Again, b_{03} cannot be half an integer.

Suppose $c = k/4$ with k odd. Clearly, b_{00} cannot possibly be integral.

The case $c = k/8$, k odd, is also impossible.

We now show that if either condition a) or b) holds, the matrix (b_{ij}) is semi-integral.

For the first part of condition b), we have $c = k/4$, $k \equiv 3 \bmod 4$, $\delta > 0$. We may take

$$V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$ For the second part we have $k \equiv 1 \bmod 4$, $\delta = 1$, and $\lambda \equiv 0 \bmod 8$. We take

$$V = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

For condition a) with c in Z, we take $V = (0)$.

Let $\mathcal{M}$ be a module of integers with norm-form $\mathcal{F}$. However, $\mathcal{M}$ is not a ring in all the instances listed in Theorems 2, 3, and 4. The next three theorems give the conditions under which $\mathcal{M}$ is a ring.

Theorem 5: Let f be of type i). $\mathcal{M}$ is a ring if and only if one of conditions a), b), or c) holds.

a) c is in Z.

b) $c = k/2$ with k odd, $a_1 = 0$, and $a_2 = 1$.

c) $c = k/4$ with $k \equiv 3 \bmod 4$, or

$$k \equiv 1 \bmod 4 \text{ and } \begin{cases} a_1 = a_2 = a_3 = 0 \\ a_1 = a_2 = 0,\ a_3 = 1, \\ \qquad m_1 m_2 \equiv 1 \bmod 4 \\ a_1 = a_2 = 0,\ a_3 \geq 1, \\ \qquad m_1 m_2 \equiv 3 \bmod 4 \end{cases}.$$

Theorem 6: Let f be of type ii). $\mathcal{M}$ is a ring if and only if one of conditions a) or b) holds.

a) c is in Z.

b) $c = k/4$ with $k \equiv 3 \bmod 4$.

Theorem 7: Let f be of type iii). $\mathcal{M}$ is a ring if and only if one of conditions a) or b) holds.

a) c is in Z.

b) $c = k/4$ with $k \equiv 3 \bmod 4$, $\delta > 0$, or

$k \equiv 1 \bmod 4$, $\delta = 1$, and $\lambda \equiv 0 \bmod 8$.

Proof of Theorem 5: Here we take $f = 2^{a_1}m_1x_1^2 + 2^{a_2}m_2x_2^2 + 2^{a_3}m_3x_3^2$, $0 \leq a_1 \leq a_2 \leq a_3$, m_i odd for $i = 1,2,3$. Then

$$a = \begin{bmatrix} 2^{a_1}m_1 & 0 & 0 \\ 0 & 2^{a_2}m_2 & 0 \\ 0 & 0 & 2^{a_3}m_3 \end{bmatrix} \text{ and}$$

$$A = \begin{bmatrix} 2^{a_2+a_3}m_2m_3 & 0 & 0 \\ 0 & 2^{a_1+a_3}m_1m_3 & 0 \\ 0 & 0 & 2^{a_1+a_2}m_1m_2 \end{bmatrix}.$$

The quaternion algebra associated with the form f has four basal elements $1, k_1, k_2, k_3$ which satisfy the multiplication table

$$k_1^2 = -2^{a_2+a_3}m_2m_3, \quad k_2^2 = -2^{a_1+a_3}m_1m_3, \quad k_3^2 = -2^{a_1+a_2}m_1m_2,$$

$$k_1k_2 = 2^{a_3}m_3k_3, \quad k_1k_3 = -2^{a_2}m_2k_2, \quad k_2k_3 = 2^{a_1}m_1k_1,$$

and $k_rk_s = -k_sk_r$ for $r,s = 1, 2, 3$.

The module $\mathfrak{N}$ which has $F + cF$ for its norm-form has $1, k_1, \ldots, k_7$ for a $\mathbb{Z}$-basis where $k_4^2 = -c$, $k_5 = k_1k_4$, $k_6 = k_2k_4$, $k_7 = k_3k_4$.

For $c = k/4$, $k \equiv 3 \bmod 4$ we have

$V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ and therefore $\mathcal{M}$ has for a Z-basis $1, e_1, \ldots, e_7$ where $e_1 = k_1$, $e_2 = k_2$, $e_3 = k_3$, $e_4 = 1/2 + k_4$, $e_5 = k_1/2 + k_5$, $e_6 = k_2/2 + k_6$, $e_7 = k_3/2 + k_7$.

For $c = k/4$, $k \equiv 1 \bmod 4$, $\alpha_1 = \alpha_2 = \alpha_3 = 0$ we have $V = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$ and $1, e_1 = k_1, e_2 = k_2, e_3 = k_3, e_4 = (k_1 + k_2 + k_3)/2 + k_4, e_5 = (1 + k_2 + k_3)/2 + k_5, e_6 = (1 + k_1 + k_3)/2 + k_6, e_7 = (1 + k_1 + k_2)/2 + k_7$ for a Z-basis for $\mathcal{M}$. Let $\alpha_1 = \alpha_2 = 0$. Then

$V = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$, if $\alpha_3 \geq 1$, $m_1 m_2 \equiv 3 \bmod 4$,

and $V = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$, if $\alpha_3 = 1$, $m_1 m_2 \equiv 1 \bmod 4$,

give $1, e_1 = k_1, e_2 = k_2, e_3 = k_3, e_4 = k_3/2 + k_4, e_5 = k_2/2 + k_5, e_6 = k_1/2 + k_6, e_7 = 1/2 + k_7$ and

$1, e_1 = k_1, e_2 = k_2, e_3 = k_3, e_4 = (k_2 + k_3)/2 + k_4,$
$e_5 = k_2/2 + k_5, e_6 = k_1/2 + k_6, e_7 = (1 + k_1)/2 + k_7$
respectively as Z-bases of $\mathcal{M}$.

For $c = k/2$, k odd, $\alpha_1 = 0$, $\alpha_2 = 1$ we have

$$V = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$ which gives us $1, e_1 = k_1,$

$e_2 = k_2, e_3 = k_3, e_4 = k_3/2 + k_4, e_5 = k_5, e_6 = k_1/2 + k_6,$
$e_7 = k_7$ for a Z-basis of $\mathcal{M}$.

For c integral we take V = (0) which gives us $1, k_1, \ldots, k_7$ as a Z-basis of $\mathcal{M}$.

For all the above cases we can verify that $\mathcal{M}$ is closed under multiplication.

The only instance where $\mathcal{M}$ is not a ring is where f is of type i), $c = k/4$ with $k \equiv 1 \bmod 4$, $\alpha_1 = 0$, $\alpha_2 = 1$, $\alpha_3 \geq 1$. We now show that under the above conditions $\mathcal{M}$ is not closed under multiplication.

For the case $c = k/4$, $k \equiv 1 \bmod 4$, $\alpha_1 = 0$, $\alpha_2 = 1$, $\alpha_3 = 1$, we have only two possibilities for the matrix V. They are

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ v_{10} & v_{11} & v_{12} & v_{13} \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ v_{10} & v_{11} & v_{12} & v_{13} \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} .$$

For either possibility we have $e_4 = (1 + v_{10}k_1 + k_3)/2 + k_4$. For the product e_1e_4 we have

$$e_1e_4 = (k_1 + v_{10}k_1^2 + k_1k_3) + k_1k_4$$

$$= k_1/2 - 2m_2m_3v_{10} - m_2k_2 + k_5$$

$$= k_1/2 - 2m_2m_3v_{10} - m_2k_2 + e_5 - v_{11}k_1/2 - k_2/2 - k_3/2$$

since $e_5 = (v_{11}k_1 + k_2 + k_3)/2 + k_5$ for either case. But $k_3/2$ is not in $\mathcal{M}$, hence e_1e_4 is not in $\mathcal{M}$, and $\mathcal{M}$ is not a ring.

Also, for the case $c = k/4$, $k \equiv 1 \bmod 4$, $\alpha_1 = 0$, $\alpha_2 = 1$, $\alpha_3 > 1$, we have $V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ v_{10} & v_{11} & 1 & v_{13} \\ v_{20} & 1 & v_{22} & v_{23} \\ 1 & 0 & 0 & 0 \end{bmatrix}$.

For a Z-basis we have 1, $e_1 = k_1$, $e_2 = k_2$, $e_3 = k_3$, $e_4 = (1 + v_{10}k_1 + v_{20}k_2 + k_3)/2 + k_4$, $e_5 = (v_{11}k_1 + k_2)/2 + k_5$, $e_6 = (k_1 + v_{22}k_2)/2 + k_6$, $e_7 = (v_{13}k_1 + v_{23}k_2 + k_3)/2 + k_7$.

$$e_1e_4 = (k_1 - 2^{\alpha_3}m_2k_2)/2 + k_5 + v_{20}2^{\alpha_3-1}m_3k_3 - v_{10}2^{\alpha_3}m_2m_3.$$

But $(k_1 - 2m_2k_2)/2 + k_5$ is not in $\mathcal{M}$ since if it were, we would have $k_2/2$ in $\mathcal{M}$ which is a contradiction. Hence, $\mathcal{M}$ is not a ring.

Proof of Theorem 6: Here we have $f = 2^{\beta+2}(jx_1^2 + x_1x_2 + jx_2^2) + 2^{\alpha}mx_3^2$, $\beta \geq 0$, $0 \leq \alpha \leq \beta$, $j = 0$ or 1. Then

$$a = \begin{bmatrix} 2^{\beta+2}j & 2^{\beta+1} & 0 \\ 2^{\beta+1} & 2^{\beta+2}j & 0 \\ 0 & 0 & 2^{\alpha}m \end{bmatrix} \quad \text{and}$$

$$A = \begin{bmatrix} 2^{\alpha+\beta+2}mj & -2^{\alpha+\beta+1}m & 0 \\ -2^{\alpha+\beta+1} & 2^{\alpha+\beta+2}mj & 0 \\ 0 & 0 & 2^{2(\beta+1)}(4j^2 - 1) \end{bmatrix}.$$

The quaternion algebra associated with the form f has four basal elements $1, k_1, k_2, k_3, k_4$ which satisfy the multiplication table

$$k_1^2 = -2^{\alpha+\beta+2}mj, \quad k_2^2 = -2^{\alpha+\beta+2}mj; \quad k_3^2 = -2^{2(\beta+1)}(4j^2 - 1),$$

$$k_2k_3 = 2^{\beta+2}jk_1 + 2^{\beta+1}k_2, \qquad k_3k_2 = -k_2k_3$$

$$k_1k_2 = 2^{\alpha+\beta+1}m + 2^{\alpha}mk_3, \qquad k_2k_1 = 2^{\alpha+\beta+1}m - 2^{\alpha}mk_3,$$

$$k_1k_3 = 2^{\beta+1}k_1 + 2^{\beta+2}jk_2, \qquad k_3k_1 = -k_1k_3.$$

The module $\mathcal{N}$ whose norm-form is F + cF has a Z-basis $1, k_1, \ldots, k_7$ where $k_4^2 = -c$, $k_5 = k_1k_4$, $k_6 = k_2k_4$, $k_7 = k_3k_4$.

For $c = k/4$, $k \equiv 3 \bmod 4$ we have

$$V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$ which gives 1, $e_1 = k_1$, $e_2 = k_2$, $e_3 = k_3$, $e_4 = 1/2 + k_4$, $e_5 = k_1/2 + k_5$, $e_6 = k_2/2 + k_6$, $e_7 = k_3/2 + k_7$ for a Z-basis of $\mathcal{M}$.

For c integral, we have V = (0) and $1, k_1, \ldots, k_7$ for a Z-basis of $\mathcal{M}$.

In either case it can be verified that $\mathcal{M}$ is a ring.

Proof of Theorem 7: Here we have $f = 2^{\delta}(jx_1^2 + x_1x_2 + jx_2^2 + \lambda x_3^2)$, $\delta \geq 0$, λ even if $j = 1$. Then

$$a = \begin{bmatrix} 2^{\delta}j & 2^{\delta-1} & 0 \\ 2^{\delta-1} & 2^{\delta}j & 0 \\ 0 & 0 & 2^{\delta}\lambda \end{bmatrix}$$ and

$$A = \begin{bmatrix} 2^{2\delta}\lambda j & -2^{2\delta-1}\lambda & 0 \\ -2^{2\delta-1}\lambda & 2^{2\delta}\lambda j & 0 \\ 0 & 0 & 2^{2(\delta-1)}(4j^2 - 1) \end{bmatrix}.$$

The quaternion algebra associated with the form f has four basal elements which satisfy the multiplication table

$$k_1^2 = -2^{2\delta}\lambda j, \quad k_2^2 = -2^{2\delta}\lambda j, \quad k_3^2 = -2^{2(\delta-1)}(4j^2 - 1),$$

$$k_2k_3 = 2^{\delta}jk_1 + 2^{\delta-1}k_2, \qquad k_3k_2 = -k_2k_3$$

$$k_1k_3 = 2^{\delta-1}k_1 + 2^{\delta}jk_2, \qquad k_3k_1 = -k_1k_3,$$

$$k_1k_2 = 2^{2\delta-1}\lambda + 2^{\delta}\lambda k_3, \qquad k_2k_1 = 2^{2\delta-1}\lambda - 2^{\delta}\lambda k_3.$$

The module $\mathcal{M}$ whose norm-form is F + cF has a Z-basis $1, k_1, \ldots, k_7$ where $k_4^2 = -c$, $k_5 = k_1k_4$, $k_6 = k_2k_4$, $k_7 = k_3k_4$.

For $c = k/4$ with $k \equiv 3 \bmod 4$ we again have

$$V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$ which gives $1, e_1 = k_1,$

$e_2 = k_2$, $e_3 = k_3$, $e_4 = 1/2 + k_4$, $e_5 = k_1/2 + k_5$, $e_6 = k_2/2 + k_6$, $e_7 = k_3/2 + k_7$ for a Z-basis of $\mathcal{M}$.

For the case $k \equiv 1 \bmod 4$, $\delta = 1$, and $\lambda \equiv 0 \bmod 8$,

we have $V = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$ giving $1, e_1 = k_1,$

$e_2 = k_2$, $e_3 = k_3$, $e_4 = k_3/2 + k_4$, $e_5 = k_1/2 + k_5$,

$e_6 = k_2/2 + k_6$, $e_7 = 1/2 + k_7$ as a Z-basis of $\mathcal{M}$.

For c integral we take V = (0) and 1, k_1, ... , k_7 is a Z-basis of $\mathcal{M}$.

In the above cases we can verify that $\mathcal{M}$ is a ring.

We now return to the case of odd primes and show that it is not possible to find a translation taking F + cF into an integral form where $c = a/p^n$, $n > 0$, a prime to p, and F as in Theorem 1.

Let us consider a translation matrix

$$T = \begin{bmatrix} I_4 & 1/p \cdot V \\ 0 & I_4 \end{bmatrix}$$ where $V = (v_{ij})$ has elements 0, 1, ... , p-1. Applying T to F + cF we obtain

$$\begin{bmatrix} F_* & 1/p \cdot F_* V \\ 1/p \cdot V' F_* & 1/p^2 \cdot V' F_* V + a/p^n \cdot F_* \end{bmatrix}.$$

Now $1/p \cdot V' F_*$, $1/p \cdot F_* V$, and $(b_{ij}) = 1/p^2 \cdot V' F_* V + a/p^n \cdot F_*$ must be integral matrices.

$$1/p \begin{bmatrix} v_{00} & v_{10} & v_{20} & v_{30} \\ v_{01} & v_{11} & v_{21} & v_{31} \\ v_{02} & v_{12} & v_{22} & v_{32} \\ v_{03} & v_{13} & v_{23} & v_{33} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p^{a_2+a_3 m_2 m_3} & 0 & 0 \\ 0 & 0 & p^{a_1+a_3 m_1 m_3} & 0 \\ 0 & 0 & 0 & p^{a_1+a_2 m_1 m_2} \end{bmatrix}$$

is equal to $1/p \cdot V' F_*$. Therefore, v_{00}, v_{01}, v_{02}, $v_{03} = 0$.

If $\alpha_1 = \alpha_2 = \alpha_3 = 0$, then $V = (0)$.

If b_{00} is to be integral, we must have

$$v_{00}^2 + p^{\alpha_2+\alpha_3} m_2 m_3 v_{10}^2 + p^{\alpha_1+\alpha_3} m_1 m_3 v_{20}^2 + p^{\alpha_1+\alpha_2} m_1 m_2 v_{30}^2 + a/p^{n-2} \equiv 0 \bmod p^2.$$

This condition cannot possibly be satisfied if $\alpha_1 > 0$ or $\alpha_1 = 0$ and $\alpha_2 > 0$.

If $\alpha_1 = 0, \alpha_2 = 0, \alpha_3 > 0$, the integrality condition for b_{00} reduces to $m_1 m_2 v_{30}^2 + a/p^{n-2} \equiv 0 \bmod p$. This is impossible if $n \geq 2$ since v_{30} must be zero. Thus, we have only the case $n = 1$ to consider. If $\alpha_3 > 1$, we have $ap \equiv 0 \bmod p^2$ which is impossible. Suppose now that $\alpha_3 = 1$. The integrality conditions for b_{00}, b_{11}, b_{01} reduce to

$$v_{10}^2 m_2 m_3 + v_{20}^2 m_1 m_3 + a \equiv 0 \bmod p,$$

$$v_{11}^2 m_2 m_3 + v_{21}^2 m_1 m_3 \equiv 0 \bmod p,$$

$$v_{10} v_{11} m_2 m_3 + v_{20} v_{21} m_1 m_3 \equiv 0 \bmod p.$$

These three conditions imply that $a \equiv 0 \bmod p$ which is a contradiction.

CHAPTER III

Given a module $\mathcal{M}$ of integers over the ring Z/p^t with norm-form $\mathcal{F}$, we now obtain conditions on $\mathcal{F}$ in order that $\mathcal{M}$ possess an isomorph (in the module sense) which is a ring.

We first consider the case of odd primes. If p is an odd prime, we have $\mathcal{F}$ equivalent to a form

$$(4) \qquad x_0^2 + m_1 p^{a_1} x_1^2 + \ldots + m_7 p^{a_7} x_7^2$$

where $0 \leq a_1 \leq \ldots \leq a_7$, m_i is either 1 or ν (ν a quadratic non-residue of p). Since the determinant of (4) is a fourth power, we have $(m_1 \ldots m_7/p) = 1$ and $\sum_{i=1}^{7} a_i$ is a multiple of 4. Examining the possibilities for the m_i and the a_i it can be verified that we may rearrange (4) as

$$(5) \qquad y_0^2 + n_1 p^{\beta_1} y_1^2 + \ldots + n_7 p^{\beta_7} y_7^2$$

where $0 \leq \beta_1 \leq \beta_2 \leq \beta_3$, $(n_1 n_2 n_3/p) = 1$, and $\beta_1 + \beta_2 + \beta_3$ is even. In other words, we may write (4) in the form F + G where the determinant of F is a square. If we consider the natural multiplication table associated with F + G, the module of integers whose norm-form is F + G cannot be a ring unless F is a Brandt

norm-form and G satisfies certain other properties. In this chapter we shall prove the preceding statement and determine conditions on G so that the module whose norm-form is F + G is a ring.

<u>Theorem 8</u>: Let $\mathcal{M}$ be a module of integers over Z/p^t with norm-form $\mathcal{F}$ which is equivalent to a form

$$\mathcal{F}' = x_0^2 + m_1 p^{a_1} x_1^2 + \ldots + m_7 p^{a_7} x_7^2$$

where $0 \leq a_1 \leq \ldots \leq a_7$ and m_i is either 1 or ν. If $\mathcal{M}'$ is the isomorph of $\mathcal{M}$ whose norm-form is $\mathcal{F}'$ and if $\mathcal{F}'$ possesses an isomorphic module which is a ring, we may rewrite $\mathcal{F}'$ as F + G where F is a Brandt norm-form.

Proof: From the previous remarks we can always rewrite $\mathcal{F}'$ as F + G where the determinant of F is a square. Consider a rearrangement of $\mathcal{F}'$ in the form F + G so that F is not a Brandt norm-form. That is, $F = y_0^2 + n_1 p^{\beta_1} y_1^2 + n_2 p^{\beta_2} y_2^2 + n_3 p^{\beta_3} y_3^2$, $0 \leq \beta_1 \leq \beta_2 \leq \beta_3$, we have $(n_1 n_2 n_3/p) = 1$, $\beta_1 + \beta_2 + \beta_3$ even, but $\beta_3 > \beta_1 + \beta_2$. We obtain a set of basal elements corresponding to the module whose norm-form is F + F and by transforming F into G obtain a set of basal elements of the module whose norm-form is F + G. We may write F as y_0^2 + adj f where

adj $f = n_1 p^{\beta_1} y_1^2 + n_2 p^{\beta_2} y_2^2 + n_3 p^{\beta_3} y_3^2$. Then

$$f = s_1 p^{\frac{\beta_2+\beta_3-\beta_1}{2}} y_1^2 + s_2 p^{\frac{\beta_1+\beta_3-\beta_2}{2}} y_2^2 + s_3 p^{\frac{\beta_1+\beta_2-\beta_3}{2}} y_3^2,$$

where $s_1 s_2 = n_3$, $s_1 s_3 = n_2$, and $s_2 s_3 = n_1$.

Corresponding to F (or f) we have the four basal elements $1, j_1, j_2, j_3$ where

$$j_1^2 = -n_1 p^{\beta_1}, \quad j_2^2 = -n_2 p^{\beta_2}, \quad j_3^2 = -n_3 p^{\beta_3},$$

$$j_1 j_2 = s_3 p^{\frac{\beta_1+\beta_2-\beta_3}{2}} j_3, \qquad j_2 j_1 = -j_1 j_2$$

$$j_2 j_3 = s_1 p^{\frac{\beta_2+\beta_3-\beta_1}{2}} j_1, \qquad j_3 j_2 = -j_2 j_3$$

$$j_3 j_1 = s_2 p^{\frac{\beta_1+\beta_3-\beta_2}{2}} j_2, \qquad j_1 j_3 = -j_3 j_1,$$

Since $\beta_3 > \beta_1 + \beta_2$, $j_1 j_2$ is not in the module whose norm-form is F + F. If for every rearrangement of $\mathcal{F}'$ in the form F + G, F is not a Brandt norm-form, then $\mathcal{M}'$ cannot possess an isomorphic module which is a ring. This contradicts the hypothesis of the theorem.

Changing the notation slightly, we shall write $\mathcal{F}'$ in the form F + cG where c is in Z. We now show that F and G are p-adically equivalent for odd primes.

Now

$$c_p(\mathcal{F}') = c_p(F + cG)$$

$$= (-1,-1)_p(d_1,d_2)_p c_p(F)c_p(cG)$$

$$= c_p(F)c_p(cG)$$

where d_1 and d_2 denote the determinants of F and cG respectively. Moreover, d_1 and d_2 are squares. Also

$$c_p(cG) = (c,d_2')_p c_p(G)$$

$$= c_p(G)$$

where d_2' denotes the determinant of G which is a square. Therefore, $c_p(\mathcal{F}') = c_p(F)c_p(G) = 1$. Hence, $c_p(F) = c_p(G) = 1$ or -1. It is clear that $d_1 = t^2 d_2$ for some t and the number of variables is the same for each form.

We adopt here a shorthand notation for diagonal forms. For the form $x_0^2 + m_1p^{\beta_1}x_1^2 + m_2p^{\beta_2}x_2^2 + m_3p^{\beta_3}x_3^2$, we shall write $\langle 1, m_1p^{\beta_1}, m_2p^{\beta_2}, m_3p^{\beta_3}\rangle$. To denote rational p-adic equivalence of two forms F and G, we shall employ the symbol "$\sim$" and write $F \sim G$.

Again, let $\mathcal{M}$ be a module of integers over Z/p^t with norm-form $\mathcal{F}$. As we have seen before,

$\mathcal{F}$ is equivalent to a form $\mathcal{F}'$ of the type (4). Let $\mathcal{M}'$ be the isomorph of $\mathcal{M}$ whose norm-form is $\mathcal{F}'$. By Theorem 8 we may write $\mathcal{F}' = F + cG$ where F is a Brandt norm-form, c is in Z, and $F \sim G$. That is, $F = \langle 1, m_1 p^{\beta_1}, m_2 p^{\beta_2}, m_3 p^{\beta_3} \rangle$ where $\beta_1 + \beta_2 + \beta_3$ is even, $(m_1 m_2 m_3/p) = 1$, and $\beta_1 + \beta_2 \geq \beta_3$, $\beta_1 + \beta_3 \geq \beta_2$, $\beta_2 + \beta_3 \geq \beta_1$; $G = \langle 1, n_1 p^{\gamma_1}, n_2 p^{\gamma_2}, n_3 p^{\gamma_3} \rangle$ where $\gamma_1 + \gamma_2 + \gamma_3$ is even and $(n_1 n_2 n_3/p) = 1$; $c = mp^{\delta}$, $\delta \geq 0$, $m = 1$ or ν.

F and G are both rationally equivalent to one of the following forms:

$\langle 1, 1, 1, 1 \rangle$	$c_p = 1$
$\langle 1, 1, \nu, \nu \rangle$	$c_p = 1$
$\langle 1, 1, p, p \rangle$	$c_p = (-1/p)$
$\langle 1, \nu, \nu p, p \rangle$	$c_p = -(-1/p)$
$\langle 1, 1, \nu p, \nu p \rangle$	$c_p = (-1/p)$.

Using the fact $c_p(F) = c_p(G)$, we have the following 21 possible combinations:

	$F \sim$	$G \sim$
For any p	$\langle 1, 1, 1, 1 \rangle$	$\langle 1, 1, 1, 1 \rangle$
	$\langle 1, 1, \nu, \nu \rangle$	$\langle 1, 1, \nu, \nu \rangle$
	$\langle 1, 1, p, p \rangle$	$\langle 1, 1, p, p \rangle$
	$\langle 1, \nu, \nu p, p \rangle$	$\langle 1, \nu, \nu p, p \rangle$

$\langle 1, 1, \nu p, \nu p\rangle$	$\langle 1, 1, \nu p, \nu p\rangle$
$\langle 1, 1, 1, 1\rangle$	$\langle 1, 1, \nu, \nu\rangle$
$\langle 1, 1, \nu, \nu\rangle$	$\langle 1, 1, 1, 1\rangle$
$\langle 1, 1, p, p\rangle$	$\langle 1, 1, \nu p, \nu p\rangle$
$\langle 1, 1, \nu p, \nu p\rangle$	$\langle 1, 1, p, p\rangle$

For $p \equiv 1 \bmod 4$

$\langle 1, 1, 1, 1\rangle$	$\langle 1, 1, p, p\rangle$
$\langle 1, 1, \nu, \nu\rangle$	$\langle 1, 1, \nu p, \nu p\rangle$
$\langle 1, 1, p, p\rangle$	$\langle 1, 1, 1, 1\rangle$
$\langle 1, 1, \nu p, \nu p\rangle$	$\langle 1, 1, \nu, \nu\rangle$
$\langle 1, 1, \nu, \nu\rangle$	$\langle 1, 1, p, p\rangle$
$\langle 1, 1, p, p\rangle$	$\langle 1, 1, \nu, \nu\rangle$
$\langle 1, 1, 1, 1\rangle$	$\langle 1, 1, \nu p, \nu p\rangle$
$\langle 1, 1, \nu p, \nu p\rangle$	$\langle 1, 1, 1, 1\rangle$

For $p \equiv 3 \bmod 4$

$\langle 1, 1, 1, 1\rangle$	$\langle 1, \nu, \nu p, p\rangle$
$\langle 1, \nu, \nu p, p\rangle$	$\langle 1, 1, 1, 1\rangle$
$\langle 1, 1, \nu, \nu\rangle$	$\langle 1, \nu, \nu p, p\rangle$
$\langle 1, \nu, \nu p, p\rangle$	$\langle 1, 1, \nu, \nu\rangle$

Given a norm-form $\mathcal{F}' = F + cG$, F and G are rationally equivalent to one of the preceding 21 pairs. We now determine necessary and sufficient conditions that $\mathcal{F}' = F + cG$, F a Brandt norm-form, be the norm-form of a ring.

We first obtain a Z-basis $j = (1, j_1, \ldots, j_7)$ for the module $\mathcal{N}$ whose norm-form is F + cF. If T denotes the matrix of the transformation carrying F into G, then $k = (1, k_1, \ldots, k_7) = j \cdot T$ is a Z-basis of the module $\mathcal{M}'$ whose norm-form is $\mathcal{F}'$. We then write out expressions for all products $k_r k_s$, $r,s = 1, \ldots, 7$ and determine the necessary and sufficient conditions that $\mathcal{M}'$ be closed under multiplication.

Theorem 9: Let p be any odd prime and suppose

F ~	G ~
⟨1, 1, 1, 1⟩	⟨1, 1, 1, 1⟩
⟨1, 1, ν, ν⟩	⟨1, 1, ν, ν⟩
⟨1, 1, p, p⟩	⟨1, 1, p, p⟩
⟨1, ν, νp, p⟩	⟨1, ν, νp, p⟩
⟨1, 1, νp, νp⟩	⟨1, 1, νp, νp⟩

If $\gamma_1 \equiv \beta_1 \bmod 2$, $\gamma_2 \equiv \beta_2 \bmod 2$, and $\gamma_3 \equiv \beta_3 \bmod 2$, the matrix of the transformation which takes F into G is

$$T_* = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p^{\frac{\gamma_1-\beta_1}{2}} & 0 & 0 \\ 0 & 0 & p^{\frac{\gamma_2-\beta_2}{2}} & 0 \\ 0 & 0 & 0 & p^{\frac{\gamma_3-\beta_3}{2}} \end{bmatrix}.$$ The following

are necessary and sufficient conditions for F + cG

to be the norm-form of a ring: $\beta_1 \geq \gamma_1$, $\beta_2 \geq \gamma_2$, $\beta_3 \geq \gamma_3$.

Proof: Suppose the module of integers whose norm-form is F + cG is a ring. The module whose norm-form is F + cG has a Z-basis $1, j_1, \ldots, j_7$ where

$$j_1^2 = -m_1 p^{\beta_1}, \quad j_2^2 = -m_2 p^{\beta_2}, \quad j_3^2 = -m_3 p^{\beta_3},$$

$$j_1 j_2 = s_3 p^{\frac{\beta_1+\beta_2-\beta_3}{2}} j_3, \qquad j_2 j_1 = -j_1 j_2$$

$$j_2 j_3 = s_1 p^{\frac{\beta_2+\beta_3-\beta_1}{2}} j_1, \qquad j_3 j_2 = -j_2 j_3$$

$$j_3 j_1 = s_2 p^{\frac{\beta_1+\beta_3-\beta_2}{2}} j_2, \qquad j_1 j_3 = -j_3 j_1$$

and $s_1 s_2 = m_3$, $s_1 s_3 = m_2$, $s_2 s_3 = m_1$,

$$j_4^2 = -c = -mp^{\delta}, \; j_5 = j_1 j_4, \; j_6 = j_2 j_4, \; j_7 = j_3 j_4 .$$

By transforming F + cF into F + cG with a transformation whose matrix is $\begin{bmatrix} I_4 & 0 \\ 0 & T_* \end{bmatrix}$ we obtain a set of basal elements $1, k_1, \ldots, k_7$ for the module whose norm-form is F + cG where

$$k_1 = j_1, \; k_2 = j_2, \; k_3 = j_3, \; k_4 = j_4,$$

$$k_5 = p^{\frac{\gamma_1-\beta_1}{2}} j_5, \; k_6 = p^{\frac{\gamma_2-\beta_2}{2}} j_6, \; k_7 = p^{\frac{\gamma_3-\beta_3}{2}} j_7.$$

To within a sign, we have

$$k_1k_4 = j_1j_4 = j_5 = p^{\frac{\beta_1-\gamma_1}{2}} k_5$$

$$k_2k_4 = j_2j_4 = j_6 = p^{\frac{\beta_2-\gamma_2}{2}} k_6$$

$$k_3k_4 = j_3j_4 = p^{\frac{\beta_3-\gamma_3}{2}} k_7$$

$$k_4^2 = mp^{\delta}$$

$$k_4k_5 = j_1k_4^2 = mp^{\delta}j_1 = mp^{\delta}k_1$$

$$k_4k_6 = j_2k_4^2 = mp^{\delta}j_2 = mp^{\delta}k_2$$

$$k_4k_7 = j_3k_4^2 = mp^{\delta}j_3 = mp^{\delta}k_3$$

$$k_1k_5 = m_1p^{\beta_1}j_4 = m_1p^{\beta_1}k_4$$

$$k_2k_5 = s_3p^{\frac{\beta_1+\beta_2-\beta_3}{2}} j_7 = s_3p^{\frac{\beta_1+\beta_2-\gamma_3}{2}} k_7$$

$$k_3k_5 = s_2p^{\frac{\beta_1+\beta_3-\beta_2}{2}} j_6 = s_2p^{\frac{\beta_1+\beta_3-\gamma_2}{2}} k_6$$

$$k_5^2 = mp^{\delta}m_1p^{\beta_1} = mm_1p^{\delta+\beta_1}$$

$$k_5k_6 = mp^{\delta}s_3p^{\frac{\beta_1+\beta_2-\beta_3}{2}} j_3 = ms_3p^{\frac{2\delta+\beta_1+\beta_2-\beta_3}{2}} k_3$$

$$k_6k_7 = mp\, s_2p^{\frac{\beta_1+\beta_3-\beta_2}{2}} j_2 = ms_2p^{\frac{2\delta+\beta_1+\beta_3-\beta_2}{2}} k_2$$

$$k_1k_6 = s_3p^{\frac{\beta_1+\beta_2-\beta_3}{2}} j_7 = s_3p^{\frac{\beta_1+\beta_2-\gamma_3}{2}} k_7$$

$$k_2k_6 = m_2p^{\beta_2} j_4 = m_2p^{\beta_2} k_4$$

$$k_3k_6 = m_2p^{\frac{\beta_2+\beta_3-\beta_1}{2}} j_5 = s_1p^{\frac{\beta_2+\beta_3-\gamma_1}{2}} k_5$$

$$k_6^2 = mp^{\delta} m_2p^{\beta_2} = mm_2p^{\delta+\beta_2}$$

$$k_6k_7 = mp^{\delta} s_1p^{\frac{\beta_2+\beta_3-\beta_1}{2}} j_1 = ms_1p^{\frac{2\delta+\beta_2+\beta_3-\beta_1}{2}} k_1$$

$$k_1k_7 = s_2p^{\frac{\beta_1+\beta_3-\beta_2}{2}} j_6 = s_2p^{\frac{\beta_1+\beta_3-\gamma_2}{2}} k_6$$

$$k_2k_7 = s_1p^{\frac{\beta_2+\beta_3-\beta_1}{2}} j_5 = s_1p^{\frac{\beta_2+\beta_3-\gamma_1}{2}} k_5$$

$$k_3k_7 = m_3p^{\beta_3} j_4 = m_3p^{\beta_3} k_4$$

$$k_7^2 = mp^{\delta} m_3p^{\beta_3} = mm_3p^{\delta+\beta_3}$$

Since we have assumed that the module whose norm-form is F + cG is a ring, 1, k_1, ... , k_7 is a

Z-basis and the powers of p in the preceding multiplication table must be non-negative. That is, $\beta_1 - \gamma_1 \geq 0$, $\beta_2 - \gamma_2 \geq 0$, $\beta_3 - \gamma_3 \geq 0$, $\beta_1 + \beta_2 - \gamma_3 \geq 0$, $\beta_1 + \beta_3 - \gamma_2 \geq 0$, $\beta_2 + \beta_3 - \gamma_1 \geq 0$, $2\delta + \beta_1 + \beta_2 - \beta_3 \geq 0$, $2\delta + \beta_2 + \beta_3 - \beta_1 \geq 0$, and $2\delta + \beta_1 + \beta_3 - \beta_2 \geq 0$. Since F is a Brandt norm-form, we have $\beta_1 + \beta_2 \geq \beta_3$, $\beta_2 + \beta_3 \geq \beta_1$, and $\beta_1 + \beta_3 \geq \beta_2$; and we see that the conditions $\beta_1 \geq \gamma_1$, $\beta_2 \geq \gamma_2$, $\beta_3 \geq \gamma_3$ are necessary.

If $\beta_1 \equiv \gamma_1 \bmod 2$, $\beta_2 \equiv \gamma_2 \bmod 2$, and $\beta_3 \equiv \gamma_3 \bmod 2$, the transformation whose matrix is T_* carries F into G. In view of the preceding multiplication table the conditions $\beta_1 \geq \gamma_1$, $\beta_2 \geq \gamma_2$, $\beta_3 \geq \gamma_3$ are sufficient for closure.

Theorem 10: Let p be any odd prime and suppose

	$F\sim$	$G\sim$
a)	$\langle 1, 1, 1, 1\rangle$	$\langle 1, 1, \nu, \nu\rangle$
b)	$\langle 1, 1, \nu, \nu\rangle$	$\langle 1, 1, 1, 1\rangle$
c)	$\langle 1, 1, p, p\rangle$	$\langle 1, 1, \nu p, \nu p\rangle$
d)	$\langle 1, 1, \nu p, \nu p\rangle$	$\langle 1, 1, p, p\rangle$

If $\gamma_1 \equiv \beta_1 \bmod 2$, $\gamma_2 \equiv \beta_2 \bmod 2$, and $\gamma_3 \equiv \beta_3 \bmod 2$, $\gamma_2 \equiv \beta_3 \bmod 2$, and $\gamma_3 \equiv \beta_2 \bmod 2$, the matrices of the transformations which carry F into G for the four above cases are as follows:

for a) and c) $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p^{\frac{\gamma_1-\beta_1}{2}} & 0 & 0 \\ 0 & 0 & a_p^{\frac{\gamma_2-\beta_2}{2}} & b_p^{\frac{\gamma_3-\beta_2}{2}} \\ 0 & 0 & -b_p^{\frac{\gamma_2-\beta_3}{2}} & a_p^{\frac{\gamma_3-\beta_3}{2}} \end{bmatrix}$ and

for b) and d) $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p^{\frac{\gamma_1-\beta_1}{2}} & 0 & 0 \\ 0 & 0 & \bar{\nu}_p^{a\,\frac{\gamma_2-\beta_2}{2}} & \bar{\nu}_p^{b\,\frac{\gamma_3-\beta_2}{2}} \\ 0 & 0 & -\bar{\nu}_p^{b\,\frac{\gamma_2-\beta_3}{2}} & \bar{\nu}_p^{a\,\frac{\gamma_3-\beta_3}{2}} \end{bmatrix}$ where

$a^2 + b^2 \equiv \nu \bmod p$. The following conditions are necessary and sufficient for $F + cG$ to be the norm-form of a ring:

$$\beta_1 \geq \gamma_1 \qquad 2\delta + \gamma_1 - \beta_1 \geq 0 \qquad \gamma_2 + \beta_1 - \gamma_3 \geq 0$$

$$\beta_2 \geq \gamma_2 \qquad 2\delta + \gamma_2 - \beta_2 \geq 0 \qquad \gamma_3 + \beta_1 - \gamma_2 \geq 0$$

$$\beta_3 \geq \gamma_3 \qquad 2\delta + \gamma_2 - \beta_3 \geq 0 \qquad \gamma_3 + \beta_2 - \gamma_1 \geq 0$$

$$\beta_2 \geq \gamma_3 \qquad 2\delta + \gamma_3 - \beta_2 \geq 0 \qquad \gamma_3 + \beta_3 - \gamma_1 \geq 0$$

$$\beta_3 \geq \gamma_2 \qquad 2\delta + \gamma_3 - \beta_3 \geq 0 \qquad 2\delta + \gamma_3 + \gamma_2 - \beta_1 \geq 0.$$

Proof: The proof is similar to that of Theorem 9.

The proofs of Theorems 11-15 are also similar to that of Theorem 9.

Theorem 11: Now suppose $p \equiv 1 \bmod 4$ and

	$F\sim$	$G\sim$
a)	$\langle 1, 1, 1, 1\rangle$	$\langle 1, 1, p, p\rangle$
b)	$\langle 1, 1, \nu, \nu\rangle$	$\langle 1, 1, \nu p, \nu p\rangle$
c)	$\langle 1, 1, p, p\rangle$	$\langle 1, 1, 1, 1\rangle$
d)	$\langle 1, 1, \nu p, \nu p\rangle$	$\langle 1, 1, \nu, \nu\rangle$
e)	$\langle 1, 1, \nu, \nu\rangle$	$\langle 1, 1, p, p\rangle$
f)	$\langle 1, 1, p, p\rangle$	$\langle 1, 1, \nu, \nu\rangle$
g)	$\langle 1, 1, 1, 1\rangle$	$\langle 1, 1, \nu p, \nu p\rangle$
h)	$\langle 1, 1, \nu p, \nu p\rangle$	$\langle 1, 1, 1, 1\rangle$.

If $\gamma_1 \equiv \beta_1 \bmod 2$, $\gamma_2 \not\equiv \beta_2 \bmod 2$, $\gamma_3 \not\equiv \beta_3 \bmod 2$, $\gamma_3 \not\equiv \beta_2 \bmod 2$, and $\gamma_2 \equiv \beta_3 \bmod 2$, the matrices of the transformations which carry F into G for the eight above cases are as follows:

for a), b), c), d)
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p^{\frac{\gamma_1-\beta_1}{2}} & 0 & 0 \\ 0 & 0 & rp^{\frac{\gamma_2-\beta_2-1}{2}} & sp^{\frac{\gamma_3-\beta_2-1}{2}} \\ 0 & 0 & -sp^{\frac{\gamma_2-\beta_3-1}{2}} & rp^{\frac{\gamma_3-\beta_3-1}{2}} \end{bmatrix},$$

for e), h)

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p^{\frac{\gamma_1-\beta_1}{2}} & 0 & 0 \\ 0 & 0 & \frac{(ar-sb)}{\nu}p^{\frac{\gamma_2-\beta_2-1}{2}} & \frac{(as+rb)}{\nu}p^{\frac{\gamma_3-\beta_2-1}{2}} \\ 0 & 0 & \frac{-(as+rb)}{\nu}p^{\frac{\gamma_2-\beta_3-1}{2}} & \frac{(ar-sb)}{\nu}p^{\frac{\gamma_3-\beta_3-1}{2}} \end{bmatrix},$$

and for f), g)

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p^{\frac{\gamma_1-\beta_1}{2}} & 0 & 0 \\ 0 & 0 & (ar-sb)p^{\frac{\gamma_2-\beta_2-1}{2}} & (as+rb)p^{\frac{\gamma_3-\beta_2-1}{2}} \\ 0 & 0 & -(ar+sb)p^{\frac{\gamma_2-\beta_3-1}{2}} & (ar-sb)p^{\frac{\gamma_3-\beta_3-1}{2}} \end{bmatrix},$$

where $a^2 + b^2 \equiv \nu \mod p$ and $r^2 + s^2 = p$. If $F + cG$ is to be the norm-form of a ring, it is necessary and sufficient that

$\beta_1-\gamma_1 \geq 0$ $\quad 2\delta+\gamma_1-\beta_1 \geq 0$ $\quad \gamma_2+\beta_1-\gamma_3 \geq 0$

$\beta_2-\gamma_2-1 \geq 0$ $\quad 2\delta+\gamma_2-\beta_2-1 \geq 0$ $\quad \gamma_2+\beta_2-\gamma_1-1 \geq 0$

$\beta_2-\gamma_3-1 \geq 0$ $\quad 2\delta+\gamma_2-\beta_3-1 \geq 0$ $\quad \gamma_2+\beta_3-\gamma_1-1 \geq 0$

$\beta_3-\gamma_2-1 \geq 0$ $\quad 2\delta+\gamma_3-\beta_2-1 \geq 0$ $\quad \gamma_3+\beta_1-\gamma_2 \geq 0$

$\beta_3-\gamma_3-1 \geq 0$ $\quad 2\delta+\gamma_3-\beta_3-1 \geq 0$ $\quad \gamma_3+\beta_2-\gamma_1-1 \geq 0$

$$2\delta+\gamma_3+\gamma_2-\beta_1 \geq 0 \qquad \gamma_3+\beta_3-\gamma_1-1 \geq 0$$

Theorems 12-15 deal with case $p \equiv 3 \bmod 4$.

Theorem 12: If $F \sim \langle 1, 1, 1, 1\rangle$ and $G \sim \langle 1, \nu, \nu p, p\rangle$, $\gamma_1 \equiv \beta_1 \bmod 2$, $\gamma_1 \equiv \beta_2 \bmod 2$, $\gamma_2 \not\equiv \beta_2 \bmod 2$, $\gamma_3 \not\equiv \beta_3 \bmod 2$, $\gamma_2 \not\equiv \beta_1 \bmod 2$, $\gamma_3 \not\equiv \beta_1 \bmod 2$, $\gamma_2 \not\equiv \beta_3 \bmod 2$, and $\gamma_3 \not\equiv \beta_2 \bmod 2$, the matrix of the transformation carrying F into G is

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & au\,p^{\frac{\gamma_1-\beta_1}{2}} & bru\,p^{\frac{\gamma_2-\beta_1-1}{2}} & bs\,p^{\frac{\gamma_3-\beta_1-1}{2}} \\ 0 & bu\,p^{\frac{\gamma_1-\beta_2}{2}} & -aru\,p^{\frac{\gamma_2-\beta_2-1}{2}} & -as\,p^{\frac{\gamma_3-\beta_2-1}{2}} \\ 0 & 0 & su\,p^{\frac{\gamma_2-\beta_3-1}{2}} & r\,p^{\frac{\gamma_3-\beta_3-1}{2}} \end{bmatrix}$$

where $a^2 + b^2 \equiv -1 \bmod p$, $p = r^2 - s^2$, and $-\nu \equiv u^2 \bmod p$. The following are necessary and sufficient conditions for $F + cG$ to be the norm-form of a ring:

$$\begin{array}{lll} \beta_1-\gamma_1 \geq 0 & 2\delta+\gamma_1-\beta_1 \geq 0 & \gamma_2+\beta_1-\gamma_1-1 \geq 0 \\ \beta_1-\gamma_2-1 \geq 0 & 2\delta+\gamma_1-\beta_2 \geq 0 & \gamma_2+\beta_2-\gamma_1-1 \geq 0 \\ \beta_1-\gamma_3-1 \geq 0 & 2\delta+\gamma_2-\beta_1-1 \geq 0 & \gamma_2+\beta_2-\gamma_3 \geq 0 \\ \beta_2-\gamma_1 \geq 0 & 2\delta+\gamma_2-\beta_2-1 \geq 0 & \gamma_2+\beta_3-\gamma_1-1 \geq 0 \\ \beta_2-\gamma_2-1 \geq 0 & 2\delta+\gamma_2-\beta_3-1 \geq 0 & \gamma_3+\beta_1-\gamma_1-1 \geq 0 \end{array}$$

$\beta_2-\gamma_3-1 \geq 0$ $\quad 2\delta+\gamma_3-\beta_1-1 \geq 0$ $\quad \gamma_3+\beta_1-\gamma_1-1 \geq 0$

$\beta_3-\gamma_2-1 \geq 0$ $\quad 2\delta+\gamma_3-\beta_2-1 \geq 0$ $\quad \gamma_3+\beta_1-\gamma_2 \geq 0$

$\beta_3-\gamma_3-1 \geq 0$ $\quad 2\delta+\gamma_3-\beta_3-1 \geq 0$ $\quad \gamma_3+\beta_2-\gamma_1-1 \geq 0$

$2\delta+\gamma_2+\beta_3-1 \geq 0$ $\quad \gamma_3+\beta_3-\gamma_1-1 \geq 0$.

$2\delta+\gamma_2+\beta_3-\gamma_2 \geq 0$

Theorem 13: If $F \sim \langle 1, \nu, \nu p, p\rangle$ and $G \sim \langle 1, 1, 1, 1\rangle$, $\gamma_1 \equiv \beta_1 \bmod 2$, $\gamma_2 \equiv \beta_1 \bmod 2$, $\gamma_2 \not\equiv \beta_2 \bmod 2$, $\gamma_3 \not\equiv \beta_3 \bmod 2$, $\gamma_1 \not\equiv \beta_2 \bmod 2$, $\gamma_1 \not\equiv \beta_3 \bmod 2$, $\gamma_2 \not\equiv \beta_3 \bmod 2$, and $\gamma_3 \not\equiv \beta_2 \bmod 2$, the transformation taking F into G has

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -\frac{a}{u}\, p^{\frac{\gamma_1-\beta_1}{2}} & -\frac{b}{u}\, p^{\frac{\gamma_2-\beta_1}{2}} & 0 \\ 0 & \frac{-rb}{u}\, p^{\frac{\gamma_1-\beta_2-1}{2}} & \frac{ra}{u}\, p^{\frac{\gamma_2-\beta_2-1}{2}} & -\frac{s}{u}\, p^{\frac{\gamma_3-\beta_2-1}{2}} \\ 0 & bs\, p^{\frac{\gamma_1-\beta_3-1}{2}} & -sa\, p^{\frac{\gamma_2-\beta_3-1}{2}} & r\, p^{\frac{\gamma_3-\beta_3-1}{2}} \end{bmatrix}$$

as its matrix where $a^2 + b^2 \equiv -1 \bmod p$, $p = r^2 - s^2$, and $-\nu \equiv u^2 \bmod p$. The following conditions are necessary and sufficient for $F + cG$ to be the norm-form of a ring:

$\beta_1-\gamma_1 \geq 0$ $\quad 2\delta+\gamma_1-\beta_1 \geq 0$ $\quad \gamma_2+\beta_2-\gamma_1-1 \geq 0$

$\beta_2-\gamma_2 \geq 0$ $\quad 2\delta+\gamma_1-\beta_2-1 \geq 0$ $\quad \gamma_2+\beta_3-\gamma_1-1 \geq 0$

$\beta_1-\gamma_2-1 \geq 0$ $\quad 2\delta+\gamma_1-\beta_3-1 \geq 0$ $\quad \gamma_3+\beta_2-\gamma_1-1 \geq 0$

$\beta_1-\gamma_3-1 \geq 0$ $\quad 2\delta+\gamma_2-\beta_1 \geq 0$ $\quad \gamma_3+\beta_3-\gamma_1-1 \geq 0$

$\beta_2-\gamma_2-1 \geq 0$ $\quad 2\delta+\gamma_2-\beta_2-1 \geq 0$

$\beta_2-\gamma_3-1 \geq 0$ $\quad 2\delta+\gamma_2-\beta_3-1 \geq 0$

$\beta_3-\gamma_2-1 \geq 0$ $\quad 2\delta+\gamma_3-\beta_2-1 \geq 0$

$\beta_3-\gamma_3-1 \geq 0$ $\quad 2\delta+\gamma_3-\beta_3-1 \geq 0$

Theorem 14: If $F \sim \langle 1, 1, \nu, \nu \rangle$ and $G \sim \langle 1, \nu, \nu p, p \rangle$, $\gamma_1 \equiv \beta_1 \bmod 2$, $\gamma_3 \not\equiv \beta_3 \bmod 2$, $\gamma_2 \not\equiv \beta_1 \bmod 2$, $\gamma_2 \not\equiv \beta_3 \bmod 2$, and $\gamma_3 \not\equiv \beta_1 \bmod 2$, the matrix of the transformation carrying F into G is

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & su\,p^{\frac{\gamma_2-\beta_1-1}{2}} & rp^{\frac{\gamma_3-\beta_1-1}{2}} \\ 0 & p^{\frac{\gamma_1-\beta_2}{2}} & 0 & 0 \\ 0 & 0 & rp^{\frac{\gamma_2-\beta_3-1}{2}} & \frac{s}{u}p^{\frac{\gamma_3-\beta_3-1}{2}} \end{bmatrix}$$

where $p = r^2 - s^2$ and $-\nu \equiv u^2 \bmod p$. In order that

F + cG be the norm-form of a ring, it is necessary and sufficient that

$\beta_2-\gamma_1 \geq 0$ $\quad 2\delta+\gamma_1-\beta_2 \geq 0$ $\quad \gamma_2+\beta_1-\gamma_3-1 \geq 0$ $\quad 2\gamma_2+\beta_2-\gamma_3 \geq 0.$

$2\delta+\gamma_2-\beta_1-1 \geq 0$ $\quad \gamma_2+\beta_3-\gamma_3-1 \geq 0$

$2\delta+\gamma_2-\beta_3-1 \geq 0$ $\quad \gamma_2+\beta_1-\gamma_1-1 \geq 0$

$2\delta+\gamma_3-\beta_1-1 \geq 0$ $\quad \gamma_2+\beta_3-\gamma_1-1 \geq 0$

$2\delta+\gamma_3-\beta_3-1 \geq 0$ $\quad \gamma_3+\beta_1-\gamma_2-1 \geq 0$

$\gamma_3+\beta_3-\gamma_2-1 \geq 0$

$\gamma_3+\beta_1-\gamma_1-1 \geq 0$

$\gamma_3+\beta_3-\gamma_1-1 \geq 0$

Theorem 15: If $F \sim \langle 1, \nu, \nu p, p\rangle$ and $G \sim \langle 1, 1, \nu, \nu\rangle$, if $\gamma_2 \equiv \beta_1 \bmod 2$, $\gamma_1 \not\equiv \beta_2 \bmod 2$, $\gamma_1 \not\equiv \beta_3 \bmod 2$, $\gamma_3 \not\equiv \beta_3 \bmod 2$, and $\gamma_3 \not\equiv \beta_2 \bmod 2$, the transformation carrying F into G has

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & p^{\frac{\gamma_2-\beta_1}{2}} & 0 \\ 0 & -\frac{s}{u}\, p^{\frac{\gamma_1-\beta_2-1}{2}} & 0 & r\, p^{\frac{\gamma_3-\beta_2-1}{2}} \\ 0 & r\, p^{\frac{\gamma_1-\beta_3-1}{2}} & 0 & -su\, p^{\frac{\gamma_3-\beta_3-1}{2}} \end{bmatrix}$$

for its matrix where $p = r^2 - s^2$, and $-\nu \equiv u^2 \bmod p$. If $F + cG$ is to be the norm-form of a ring, it is necessary and sufficient that

$$\beta_1 - \gamma_2 \geq 0 \qquad 2\delta + \gamma_1 - \beta_2 - 1 \geq 0 \qquad \gamma_1 + \beta_2 - \gamma_3 - 1 \geq 0 \qquad \gamma_3 + \beta_2 - \gamma_1 - 1 \geq 0$$

$$2\delta + \gamma_1 - \beta_3 - 1 \geq 0 \qquad \gamma_1 + \beta_3 - \gamma_3 - 1 \geq 0 \qquad \gamma_3 + \beta_3 - \gamma_1 - 1 \geq 0$$

$$2\delta + \gamma_3 - \beta_2 - 1 \geq 0 \qquad \gamma_1 + \beta_2 - \gamma_2 - 1 \geq 0 \qquad \gamma_3 + \beta_2 - \gamma_2 - 1 \geq 0$$

$$2\delta + \gamma_3 - \beta_3 - 1 \geq 0 \qquad \gamma_1 + \beta_3 - \gamma_2 - 1 \geq 0 \qquad \gamma_3 + \beta_3 - \gamma_2 - 1 \geq 0$$

$$2\delta + \gamma_2 - \beta_1 \geq 0 \qquad 2\gamma_1 + \beta_1 - \gamma_3 \geq 0$$

$$2\delta + \gamma_1 + \gamma_3 - \beta_1 \geq 0 \qquad 2\gamma_3 + \beta_1 - \gamma_1 \geq 0.$$

At least two of the relations $\gamma_1 + \gamma_2 \geq \gamma_3$, $\gamma_1 + \gamma_3 \geq \gamma_2$, $\gamma_2 + \gamma_3 \geq \gamma_1$ must hold. Thus, some of the conditions listed in Theorems 10-15 are redundant. Also, the author is trying to improve on the parity conditions given in Theorems 9-15.

A study of modules of integers over the ring $Z/2^t$ is now being made by the author. The procedure is somewhat more complicated than that for modules over Z/p^t where p is an odd prime. Also, the number of cases to be considered is much larger.

The author hopes to find a characterization of the modules of integers which are rings in terms of the ordinal invariants of their norm-forms. Some work has

been done in this direction, but no such characterization has yet been found.

SELECTED BIBLIOGRAPHY

1. Coxeter, H. S. M. " Integral Cayley Numbers," Duke Mathematical Journal, XIII(1946), 561-578.

2. Estes, Dennis and Pall, Gordon. " Modules and Rings in the Cayley Algebra," (To Appear).

3. Irwin, R. C. Quaternion Algebras over Algebraic Number Fields, (University of Arizona Library, Doctoral Dissertation, 1963).

4. Pall, Gordon. " On Generalized Quaternions," Transactions of the American Mathematical Society, LIX(1946), 280-332.

5. _____. " On the Order Invariants of Integral Quadratic Forms," Quarterly Journal of Mathematics, (1935), 30-51.

6. _____. " The Arithmetic Invariants of Quadratic Forms," Bulletin of the American Mathematical Society, LI(1945), 185-197.

7. Van der Blij, F. and Springer, T. A. " The Arithmetic of Octaves and of the Group G_2," Indagationes Mathematicae, (1959), 406-418.

AUTOBIOGRAPHY

John Thomas Hardy, Jr., was born October 30, 1938, in Booneville, Mississippi. He attended the public schools of Aberdeen and Tupelo, Mississippi. In September, 1956, he entered the University of Mississippi, Oxford, Mississippi, where he received his B.S. degree in Chemical Engineering in May, 1960. In September, 1960, he entered Louisiana State University as a graduate assistant and received his M.S. degree in August, 1962. He is currently a candidate for the degree of Doctor of Philosophy in the Department of Mathematics.

EXAMINATION AND THESIS REPORT

Candidate: John Thomas Hardy, Jr.

Major Field: Mathematics

Title of Thesis: Modules and Rings of Integers in the Cayley Algebra

Approved:

Gordon Pall
Major Professor and Chairman

Max Goodrich
Dean of the Graduate School

EXAMINING COMMITTEE:

James E. Keisler

L A Wade

R. Bzoch

H H Callins

Date of Examination:

May 25, 1965